

# Public Advice & Data Protection Complaints Services Training Manual



If you have any feedback about this manual or its contents, please complete the feedback form at this [link](#).

There are also a number of UK GDPR quizzes for new starters. These are designed to follow the UK GDPR & FOI module training. LCO trainers should ensure that these are sent to the new starters prior to them beginning their UK GDPR & FOI module training and it should be explained that each quiz should be completed following the completion of the relevant module that the quiz relates to. Links to the quizzes can be copied into the new starters weekly training plan when they're due to complete the relevant modules.

[UK GDPR Full Quiz](#)

[UK GDPR Full Quiz Answers](#)

[UK GDPR Module 1&2 Quiz](#)

[UK GDPR Module 1&2 Answers](#)

[UK GDPR Module 3 Quiz](#)

[UK GDPR Module 3 Answers](#)

[UK GDPR Module 4 Quiz](#)

[UK GDPR Module 4 Answers](#)

[UK GDPR Module 5 Quiz](#)

[UK GDPR Module 5 Answers](#)

[UK GDPR Module 6 Quiz](#)

[UK GDPR Module 6 Answers](#)

[UK GDPR Module 7 Quiz](#)

[UK GDPR Module 7 Answers](#)

[UK GDPR Module 8 Quiz](#)

[UK GDPR Module 8 Answers](#)

[UK GDPR Module 9 Quiz](#)

[UK GDPR Module 9 Answers](#)

[UK GDPR Module Exemptions Quiz](#)

[UK GDPR Module Exemption Answers](#)

[UK GDPR Module 10 Quiz](#)

[UK GDPR Module 10 Answers](#)

[UK GDPR Module 11 Quiz](#)

[UK GDPR Module 11 Answers](#)

[UK GDPR Module 12 Quiz](#)

[UK GDPR Module 12 Answers](#)

[FOI Quiz \(Part 1\) – Questions](#)

[FOI Quiz \(Part 1\) – Answers](#)

[FOI Quiz \(Part 2\) – Questions](#)

[FOI Quiz \(Part 2\) – Answers](#)

[FOI Quiz \(Part 3\) – Questions](#)

[FOI Quiz \(Part 3\) – Answers](#)

**Trainer Signature and date**

--

## **Website Quiz**

The importance of the ICO's website should be explained to all new starters. In the first couple of days all new starters should be sent a website quiz to be complete and return to the trainer as well as having time scheduled in their weekly training plan to complete this quiz.

[Website Quiz \(Questions\)](#)

[Website Quiz \(Answers\)](#)

### **Trainer Signature and date**

## **Knowledge Builder**

The importance of the Knowledge Builder should be explained to all new starters. In the first couple of weeks trainers should send all new starters the Knowledge Builder quiz to be complete and return. Time should be scheduled in new starters weekly training plans to complete this.

[Knowledge Builder Quiz \(Questions\)](#)

[Knowledge Builder Quiz \(Answers\)](#)

### **Trainer Signature and date**

## **4. LEGISLATION**

### **4.1. Department legislative training (PECR, FOI, EIR & AADC)**

#### **PECR**

[PECR – Department training handout](#)

[PECR – Department training – trainer notes](#)

[PECR – Desk Aid](#)

LCO trainers should book in a session with new starters to cover this training. Trainers will need to ensure they have access to a copy of the [Privacy and Electronic Communication Regulations](#).

#### **Trainer Signature and date**

--

#### **Freedom of Information & Environmental Information Regulations (FOI & EIR)**

[FOI & EIR Training PowerPoint presentation](#)

[FOI & EIR Training handout](#)

[FOI & EIR – Exemptions flowchart](#)

LCO trainers should book in a session with new starters to cover this training. Trainers will need to ensure they have access to a copy of the Freedom of Information Act and access to the Cabinet Office Code of Practice for a simple overview of the legislation is also useful - [Cabinet Office - Code of Practice](#).

Before the session, trainers should also review <https://www.whatdotheyknow.com/body/ico> and pick out some examples of case studies to discuss.

### **Trainer Signature and date**

### **Age-Appropriate Design Code (Children's Code)**

[PADPCS and the Children's Code Presentation](#)  
[Identifying complaints relating to children presentation](#)  
[The Children's Code – Procedures for Public Advice and Data Protection Complaints Services](#)

LCO trainers should book in a session with new starters to cover the two presentations listed above following new starters completing their online children's code training. Trainers should also have a copy of the third link above open to show and discuss with new starters.

### **Trainer Signature and date**

## **4.2. Further legislation quizzes**

We have created a number of quizzes to help trainees understanding of the certain legislation. LCO trainers should schedule time in new starters weekly training plans to complete these quizzes. Encourage new starters to use our website.

[Cookies Quiz – Questions](#)

[Cookies Quiz – Answers](#)

[eIDAS Quiz - Questions](#)

[eIDAS Quiz – Answers](#)

[Law Enforcement processing – Questions](#)

[Law Enforcement processing – Answers](#)

[NIS Quiz – Questions](#)

[NIS Quiz - Answers](#)

**Trainer Signature and date**

## **10.1. Inappropriate disclosures**

Managers of new starters should deliver the [Inappropriate disclosure – training presentation](#) to their new starters before they're signed off on any casework and ideally following the delivery of the 'establishing account contacts' presentation.

Managers should explain the procedure/process on ICON for reporting incidents and send trainees the [PADPCS Inappropriate Disclosure Policy](#) to read following the meeting.

### **Trainer Signature and date**

## **10.2 Keeping it Clear & Corporate Narrative**

Ensure that all new starters have been emailed and given the links for the [Keeping it Clear Guide](#) and [Corporate Narrative slideshow](#). Time should be scheduled in new starters training plan to read through these

### **Trainer Signature and date**

## **10.3. Enquiries**

### **\*Only to be completed if new starters manager includes it in master training plan\***

The following practice questions are written from an individual's perspective. Trainers should send new starters the practice questions and explain that responses should give practical advice about resolving individual concerns with the organisations, without the need to complain to the ICO.

The language should suit the customer – conversational and not legalistic.

[UK GDPR module 2 – practice question](#)

[UK GDPR module 2 – practice notes](#)

[UK GDPR module 3 – practice question](#)

[UK GDPR module 3 – practice notes](#)

[UK GDPR module 4 – practice question](#)

[UK GDPR module 4 – practice notes](#)

[UK GDPR module 5 – practice question](#)

[UK GDPR module 5 – practice notes](#)

[UK GDPR module 6 – practice question](#)

[UK GDPR module 6 – practice notes](#)

[UK GDPR module 7 – practice question](#)

[UK GDPR module 7 – practice notes](#)

[UK GDPR module 8 – practice question](#)

[UK GDPR module 8 – practice notes](#)

[UK GDPR module 9 – practice question](#)

[UK GDPR module 9 – practice notes](#)

[UK GDPR module 10 – practice question](#)

[UK GDPR module 10 – practice notes](#)

[UK GDPR module 11 – practice question](#)

[UK GDPR module 11 – practice notes](#)

[UK GDPR module 12 – practice question](#)

[UK GDPR module 12 – practice notes](#)

Further practice enquiry questions

[Practice Question 1](#)

[Practice notes 1](#)

[Practice Question 2](#)

[Practice notes 2](#)

[Practice Question 6](#)

[Practice notes 6](#)

**Trainer Signature and date**



### **10.4.1. Ways to progress a case**

LCO trainers should deliver [this presentation](#) to cover the different approaches we use when working on complaint cases. This will provide a brief overview of what terminology we use for our casework and will explore what Insufficient Information, Accountability, Outcome and further evidence cases look like.

#### **Trainer Signature and date**

--

### **10.4.3. Casework procedures and processes**

LCO trainers should deliver [this presentation](#) to cover some of the main casework procedures and processes. This presentation is designed to give new starters an overview of the processes they need to be aware of before starting casework. Time should be set aside in the new starters training plan for them to become familiar with SharePoint and where to locate our procedures and processes.

#### **Trainer Signature and date**

--

#### **10.4.4. Insufficient Information**

LCO trainers should deliver [this presentation](#) to cover what an Insufficient Information case looks like. LCO should allocate themselves a few Insufficient Information cases before the session and draft responses to these using the appropriate templates to demonstrate to the new starters. Further insufficient information cases should be identified from our queues to be allocated to the new starters.

#### **Trainer Signature and date**

#### **10.4.5. Accountability**

LCO trainers should deliver [this presentation](#) to cover progressing a case using our accountability templates. LCO trainers should allocate themselves a couple of cases they can use an accountability template for and draft their responses in notepad ready to demonstrate the full ICE360 process of checking contact points, creating documents and sending emails. This demonstration should take place after the 'Establishing account contacts' presentation has been delivered. LCO trainers should also identify further cases that accountability templates can be used for so they can allocate these to new starters.

New starters may benefit from following [this](#) step by step guide when sending out accountability templates, as well as any other correspondence from ICE360.

#### **Trainer Signature and date**

#### **10.4.6. Establishing account contacts**

LCO trainers should deliver [this presentation](#) following the accountability presentation. This presentation covers how to establish account contacts. LCO trainers should demonstrate

#### **Trainer Signature and date**

#### **10.4.7. Ways to provide an Outcome**

LCO trainers should deliver [this presentation](#) to cover examples of cases where we can provide an outcome. Following the presentation, cases where we can provide an outcome should then be identified within our queues and allocated to new starters.

**Trainer Signature and date**

#### **10.4.8. Further evidence**

LCO trainer should deliver [this presentation](#) to cover examples of cases where we should ask further evidence from the DC. Following the presentation, cases where we need to ask for further evidence should be identified across our work queues and allocated to new starters.

**Trainer Signature and date**

#### **10.4.9. Security, Disclosures and Criminal Offences**

LCO trainer should deliver [this presentation](#) to cover examples of security, disclosures and criminal offences that may be reported to us through complaints and the process for handling these.

**Trainer Signature and date**

#### **10.4.10. Whistleblowing**

LCO trainer should deliver [this presentation](#) to explain what a whistleblowing disclosure is and how to handle enquires new starters may receive via live services. This presentation should be delivered before new starters begin their helpline training. A further [trainer guide](#) for whistleblowing can be referred to whilst delivering this presentation.

## Cookies and similar technologies guidance quiz – answers with website links

The aim of this quiz is to help staff understand the law relating to cookies and similar technologies. Most of the law is contained in the Privacy and Electronic Communications Regulations 2003 (PECR). There is some essential interaction with the General Data Protection Regulation (the GDPR) as well. All the answers to these questions can be found on our website, specifically, the [Guide to PECR](#) and [Guidance on the use of cookies and similar technologies](#). Staff can point customers to these areas when they are in contact with them.

Question	Answer	Website section
<b>General PECR</b>		
What is PECR?	The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.	What are PECR? <a href="#">What are PECR?   ICO</a>
What does PECR cover?	<ul style="list-style-type: none"> <li>• Marketing by electronic means, including marketing calls, texts, emails and faxes. See the <a href="#">Electronic and telephone marketing</a> section of this guide for more information.</li> <li>• The use of <a href="#">cookies or similar technologies</a> that track information about people accessing a website or other electronic service. See the Cookies and similar technologies section of this guide for more information.</li> <li>• Security of public electronic communications services. See the <a href="#">Security of services</a> and <a href="#">Security breaches</a> sections of this guide for more information.</li> <li>• Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings. See the <a href="#">Communications networks and services</a> section of this guide for more information.</li> </ul>	What kind of areas do PECR cover? <a href="#">What are PECR?   ICO</a>

<p>What are the key concepts and definitions of PECR?</p> <p>Explain each, especially the term 'person' which is used in PECR instead of data controller.</p>	<ul style="list-style-type: none"> <li>• What are 'electronic communications'?</li> <li>• What is a 'public electronic communications network'?</li> <li>• What is a 'public electronic communications service'?</li> <li>• What is a 'service provider'?</li> <li>• What is a 'communications provider'?</li> <li>• What is a 'public communications provider'?</li> <li>• Who are 'subscribers' and 'users'?</li> <li>• Who are 'corporate subscribers' and 'individual subscribers'?</li> </ul>	<p>Key concepts and definitions</p> <p><a href="#">Key concepts and definitions   ICO</a></p>
<p>Does it include private networks?</p>	<p>No – It does not include private or restricted networks, only networks used by service providers who have members of the public as customers.</p>	<p><a href="#">Key concepts and definitions   ICO</a></p>
<p><b>Cookies and similar technologies</b></p>		
<p>What is a cookie?</p>	<p>Cookies are small pieces of information, normally consisting of just letters and numbers, which online services provide when users visit them. Software on the user's device (for example a web browser) can store cookies and send them back to the website next time they visit.</p>	<p>What is a cookie?</p> <p><a href="#">What are cookies and similar technologies?   ICO</a></p>
<p>How are cookies used?</p>	<p>Cookies are a specific technology that store information between website visits. They are used in numerous ways, such as:</p> <ul style="list-style-type: none"> <li>• remembering what's in a shopping basket when shopping for goods online;</li> <li>• supporting users to log in to a website;</li> <li>• analysing traffic to a website; or</li> <li>• tracking users' browsing behaviour.</li> </ul>	<p>How are cookies used?</p> <p><a href="#">What are cookies and similar technologies?   ICO</a></p>
<p>Why are they important?</p>		<p>This is an interpretive answer to show they have done the reading.</p>

What is a session cookie?	Cookies that expire at the end of a browser session (normally when a user exits their browser) are called 'session cookies'.	What are 'session' and 'persistent' cookies? <a href="#">What are cookies and similar technologies?   ICO</a>
What is a persistent cookie?	Cookies that can be stored for longer are called 'persistent cookies'. PECR applies to both types.	What are 'session' and 'persistent' cookies? <a href="#">What are cookies and similar technologies?   ICO</a>
What is a first party cookie?	First-party cookies are set directly by the website the user is visiting, ie the URL displayed in the browser's address bar.	What are 'first party' and 'third party' cookies? <a href="#">What are cookies and similar technologies?   ICO</a>
What is a third party cookie?	Third-party cookies are set by a domain other than the one the user is visiting. This typically occurs when the website incorporates elements from other sites, such as images, social media plugins or advertising. When the browser or other software fetches these elements from the other sites, they can set cookies as well	What are 'first party' and 'third party' cookies? <a href="#">What are cookies and similar technologies?   ICO</a>
What are similar technologies?	PECR applies to any technology that stores or accesses information on the user's device. This could include, for example, HTML5 local storage, Local Shared Objects and fingerprinting techniques.	What are 'similar technologies'? <a href="#">What are cookies and similar technologies?   ICO</a>
What is device fingerprinting?	Device fingerprinting is a technique that involves combining a set of information elements in order to uniquely identify a particular device.	Example box within above link
If a pixel tag is used in an email what Regulations of PECC apply?	Whilst the majority of electronic mail marketing is governed by Regulation 22 of PECC, where tracking pixels store information, or gain access to information stored, on a user's device Regulation 6 also applies.	Reg 6 – Cookies and similar technologies, and Reg 22 – electronic mail. <a href="#">What are cookies and similar technologies?   ICO</a>
How does PECC apply to cookies and similar technologies?	PECC does not refer to cookies by name, but Regulation 6 states:  (1) ... a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.  (2) The requirements are that the subscriber or user of that terminal equipment —	What does PECC say about cookies and similar technologies? <a href="#">What are the rules on cookies and similar technologies?   ICO</a>

	<p>(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and</p> <p>(b) has given his or her consent.</p>	
What must a 'person' setting cookies do?	<p>This means that if you use cookies you must:</p> <ul style="list-style-type: none"> <li>• say what cookies will be set;</li> <li>• explain what the cookies will do; and</li> <li>• obtain consent to store cookies on devices</li> </ul>	<a href="#">What are the rules on cookies and similar technologies?   ICO</a>
What information must a 'person' who sets cookies give to a subscriber or user?	<p>The information has to cover:</p> <ul style="list-style-type: none"> <li>• the cookies you intend to use;</li> <li>• the purposes for which you intend to use them;</li> <li>• any third parties who may also process information stored in or accessed from the user's device; and</li> <li>• the duration of any cookies you wish to set.</li> </ul>	<p>What does 'clear and comprehensive information' mean? <a href="#">What are the rules on cookies and similar technologies?   ICO</a></p>
What is a strictly necessary cookie?	<p>The 'strictly necessary' exemption means that storage of (or access to) information should be essential, rather than reasonably necessary. It is also restricted to what is essential to provide the service requested by the user. It does not cover what might be essential for any other uses that you might wish to make of that data. It is therefore clear that the strictly necessary exemption has a narrow application.</p>	<p>What is the 'strictly necessary' exemption? <a href="#">What are the rules on cookies and similar technologies?   ICO</a></p>
What activities are met by the strictly necessary exemption?	<p>A cookie used to remember the goods a user wishes to buy when they go to the checkout or add goods to their shopping basket;</p> <p>Cookies that are essential to comply with the UK GDPR's security principle for an activity the user has requested – for example in connection with online banking services</p>	<p>What activities are likely to meet the 'strictly necessary' exemption? <a href="#">What are the rules on cookies and similar technologies?   ICO</a></p>

	<p>Cookies that help ensure that the content of a page loads quickly and effectively by distributing the workload across numerous computers (this is often referred to as 'load balancing' or 'reverse proxying')</p>	
<p>Give examples of none strictly necessary cookies?</p>	<ul style="list-style-type: none"> <li>• Analytics</li> <li>• First and third party advertising</li> <li>• Tailored greetings</li> </ul>	<p>What is the 'strictly necessary' exemption? <a href="#">What are the rules on cookies and similar technologies?   ICO</a> Are analytics cookies exempt?</p>
<p>What level of consent is required for none strictly necessary cookies?</p>	<ul style="list-style-type: none"> <li>• The UK GDPR standard – Article 4(11)</li> </ul>	<p>What does 'consent' mean? <a href="#">What are the rules on cookies and similar technologies?   ICO</a></p>
<p>Does Regulation 6 cover other devices?</p>	<p>The use of cookies and similar technologies is not limited to traditional websites and web browsers. The rules in PECR apply to any technique that stores information, or accesses information stored, in the terminal equipment of the subscriber or user.</p>	<p>Do the rules only apply to websites? <a href="#">What are the rules on cookies and similar technologies?   ICO</a></p>
<p>What is the relationship between PECR and the GDPR?</p>	<p>PECR sits alongside the Data Protection Act 2018 (DPA) and the UK GDPR, and provides specific rules in relation to privacy and electronic communications. Where these rules apply, they take precedence over the DPA and the UK GDPR. This is important, because if you are setting cookies you need to consider PECR compliance first before you look to the UK GDPR.</p> <p>Additionally, PECR depends on data protection law for some of its definitions.</p>	<p>What is the relationship between PECR and the GDPR? <a href="#">How do the cookie rules relate to the GDPR?   ICO</a></p>
<p>How does the GDPR define a cookie or similar technology?</p>	<p>'online identifier'</p>	<p>What does the GDPR say about cookies? <a href="#">How do the cookie rules relate to the GDPR?   ICO</a></p>
<p>How does lawful basis in the GDPR fit in with PECR?</p>	<p>To process personal data, you must have a lawful basis. The UK GDPR has six lawful bases, of which one is consent. No lawful basis is more important than the other – the appropriate one depends on the specifics of your processing.</p> <p>However, PECR requirements are separate from, and different to, those of the UK GDPR. The simplest way to</p>	<p>How does cookie consent fit with the lawful basis requirements of the GDPR? <a href="#">How do the cookie rules relate to the GDPR?   ICO</a></p>



	<p>understand it is that if your cookies require consent under PECR, then you cannot use one of the alternative lawful bases from the GDPR to set them. If you're setting cookies, this is why you need to look to PECR first and comply with its specific rules, before considering any of the general rules in the UK GDPR</p>	
How is compliance with cookie rules achieved?	A catch all section of the guidance	How do we comply with the cookie rules? <a href="#">How do we comply with the cookie rules?   ICO</a>
Is a cookie wall compliant?	In some circumstances, this approach is inappropriate; for example, where the user or subscriber has no genuine choice but to sign up. This is because the UK GDPR says that consent must be freely given.	Can we use 'cookie walls'? <a href="#">How do we comply with the cookie rules?   ICO</a>
Can cookie consent be added to terms and conditions?	No – can't bundle consent under the GDPR	Can we use 'terms and conditions' to gain consent for cookies? <a href="#">How do we comply with the cookie rules?   ICO</a>
How is noncompliance dealt with?	<p>In cases where organisations refuse or fail to comply voluntarily the ICO has a range of options available for taking formal action where this is necessary.</p> <p>Where formal action is considered, perhaps because an organisation refuses to take steps to comply or has been involved in a particularly privacy-intrusive use of cookies without telling individuals or obtaining consent, any use of formal regulatory powers would be considered in line with the factors set out in the published Regulatory Action Policy.</p> <p>More guidance on the circumstances in which the Information Commissioner will use enforcement powers, including what is considered a 'serious infringement', can be found in the ICO's Regulatory Action Policy and associated guidance.</p> <p>The Regulatory Action Policy makes clear that any formal action must be a proportionate response to the issue it seeks to address and that monetary penalties</p>	What happens if we don't comply? <a href="#">What else do we need to consider?   ICO</a>

	<p>will be reserved for the most serious infringements of PECR.</p> <p>The ICO cannot exclude the possibility of formal action in any area. However, it is unlikely that priority for any formal action would be given to uses of cookies where there is a low level of intrusiveness and low risk of harm to individuals</p>	
How can a cookie complaint be made?	On our website in the 'Make a complaint' section.	Make complaint – cookies <a href="#">Cookies   ICO</a>

## The electronic identification and trust services (eIDAS) quiz

The aim of this quiz is to help staff understand the eIDAS regulations. All the answers to these questions can be found on our website, specifically, in the [Guide to eIDAS](#). Staff can point customers to these areas when they are in contact with them.

Question	Answer	Website section
<b>eIDAS</b>		
What does 'eIDAS' mean?	'eIDAS' is shorthand for 'electronic identification and trust services'. It refers to a range of services that help verify the identity of individuals and businesses online or the authenticity of electronic documents.	<a href="https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/">https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/</a>
What is the eIDAS Regulation?	<ul style="list-style-type: none"> <li>• The UK eIDAS Regulations set out rules for UK trust services and establishes a legal framework for the provision and effect of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.</li> <li>• Trust services increase confidence in the use of electronic transactions through mechanisms such as verifying the identity of individuals and businesses online and verifying the authenticity of electronic data e.g. documents.</li> <li>• The UK eIDAS Regulations are an amended form of the EU eIDAS Regulation and retain many aspects of the EU regulation but are tailored for use within the UK.</li> <li>• Although the UK eIDAS Regulations allows the legal effect of EU eIDAS qualified services to continue to be recognised and used in the UK, no reciprocal agreement currently exists. This means UK eIDAS Regulation qualified trust services are</li> </ul>	<a href="https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/">https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/</a>

	not automatically recognised and accepted as equivalent in the EU.	
What is the ICO's role?	The ICO has responsibility for supervision of the trust service provisions of the UK eIDAS Regulations. The ICO can grant and revoke qualified status for trust service providers established in the UK, approve or reject qualified trust services, report on security breaches, carry out audits and take enforcement action.	<a href="#">What is the eIDAS Regulation?   ICO</a>
What is a 'trust service'?	A trust service is an electronic service which helps to confirm that an online document or other electronic data is sent from a trusted source, is authentic and hasn't been tampered with. It aims to ensure legal certainty, trust and security in electronic transactions. There are five specific types of trust service covered by the Regulation: electronic signatures; electronic seals; electronic time stamps; electronic registered delivery services; and website authentication certificates.	<a href="#">Key definitions   ICO</a>
What is a 'trust service provider'?	A trust service provider is anyone who provides a trust service. This term includes both qualified and non-qualified trust service providers.	<a href="https://ico.org.uk/for-organisations/guide-to-eidas/key-definitions/">https://ico.org.uk/for-organisations/guide-to-eidas/key-definitions/</a>
What is a 'qualified trust service'?	Qualified trust services are trust services which have been assessed by an eIDAS accredited assessment body and granted qualified status by the ICO. By meeting the requirements set out in the UK eIDAS	<a href="#">Key definitions   ICO</a>

	<p>Regulation they provide a high degree of confidence and trustworthiness e.g. via stringent methods of authentication and validation of service users, adoption of strong operational security controls etc. Qualified trust services have special recognition in UK law and can only be offered by qualified trust service providers.</p>	
<p>What is a 'qualified trust service provider'?</p>	<p>A qualified trust service provider is an organisation providing qualified trust services that has been granted qualified status by the ICO. For any UK eIDAS defined qualified trust service, a trust service provider must comply with the requirements for trust service providers set out in the UK eIDAS Regulations and demonstrate their compliance via a process which involves an assessment by an eIDAS accredited assessment body and approval by the ICO.</p> <p>Following ICO approval, qualified trust service provider information and the qualified services they provides are published on a 'trusted list'.</p>	<p><a href="#">Key definitions   ICO</a></p>
<p>What is an 'electronic signature'?</p>	<p>An electronic signature is any method an individual uses to 'sign' an electronic document. This covers a wide range of measures, from the simple act of affixing text or a digital image, to more sophisticated hi-tech methods which meet specific criteria set out in the UK eIDAS Regulation for advanced or qualified electronic signatures. Electronic signatures are admissible as evidence in court.</p>	<p><a href="#">Key definitions   ICO</a></p>
<p>What are advanced and qualified electronic signature?</p>	<p>Advanced electronic signatures meet the extra requirements set out in UK eIDAS Regulation Article 26. They are required to uniquely link to the person signing the data in electronic form and can detect any changes made to the data within the document afterwards. Qualified electronic signatures have the</p>	<p><a href="#">Key definitions   ICO</a></p>

	<p>same features as advanced electronic signatures, but are created using more sophisticated technology, meet a higher standard of security, meet stricter validation criteria, and are supported by a more detailed certificate. They have the same legal effect as a handwritten signature.</p>	
<p>What is an 'electronic time stamp'?</p>	<p>An electronic time stamp proves that particular data existed at a particular time and hasn't been changed since then.</p>	<p><a href="#">Key definitions   ICO</a></p>
<p>What does an 'electronic registered delivery service' do?</p>	<p>They provide proof that information was sent and received electronically, and that it was not intercepted or altered on the way.</p>	<p><a href="#">Key definitions   ICO</a></p>
<p>If you want to gain qualified status, what must you do first?</p>	<p>If you want to gain qualified status, you must first ask a conformity assessment body to look at whether you meet the relevant UK eIDAS Regulation requirements for trust service providers and the trust service(s) you wish to provide. The conformity assessment body will conduct an assessment and produce a 'conformity assessment report' that is provided to the ICO for review.</p>	<p><a href="#">Key definitions   ICO</a></p>
<p>What does the law say about security measures?</p>	<p>The UK eIDAS Regulation sets out trust service providers' security obligations. Article 19(1) says: "Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."</p>	<p><a href="#">Security and accessibility of trust services   ICO</a></p>
<p>What more do qualified trust service providers need to do to comply</p>	<p>If you are a qualified trust service provider you also need to comply with some more specific minimum security requirements set out in article 24(2). You</p>	<p><a href="#">Security and accessibility of trust services   ICO</a></p>

<p>with their security obligations?</p>	<p>should look at these carefully as the requirements are quite specific, but in summary you need to:</p> <ul style="list-style-type: none"> <li>• employ reliable staff and subcontractors with the necessary expertise, experience and qualifications;</li> <li>• ensure staff and subcontractors have received appropriate security and data protection training;</li> <li>• use trustworthy, secure and reliable products and systems;</li> <li>• ensure your systems have appropriate access controls to protect data from unauthorised access or modification and ensure that unauthorised changes are detectable;</li> <li>• implement internal processes and procedures that support the security of the trust service and protect against forgery and theft;</li> <li>• ensure personal data is processed in line with data protection legislation.</li> </ul>	
<p>What must an organisation do if there is a breach?</p>	<p>You need to:</p> <ul style="list-style-type: none"> <li>• notify the ICO;</li> <li>• consider whether to notify your users; and consider whether to inform anyone else who might be affected.</li> </ul>	<p><a href="#">Breach reporting   ICO</a></p>
<p>When and how does an organisation notify the ICO?</p>	<ul style="list-style-type: none"> <li>• You must notify the ICO within 24 hours of becoming aware of the breach, or sooner if it's reasonable to do so. Using the online breach reporting form.</li> </ul>	<p><a href="#">Breach reporting   ICO</a></p>

<p>When and how does an organisation notify those affected?</p>	<p>If the breach is likely to adversely affect your users, you will also need to notify them of the breach without undue delay.</p> <p>You don't need to use a specific format for this. You can choose how you prefer to communicate with your customers, as long as it reaches them promptly. We advise you to include:</p> <ul style="list-style-type: none"> <li>• your name and contact details;</li> <li>• the date of the breach;</li> <li>• a summary of the incident;</li> <li>• the likely effect on them;</li> <li>• any measures you have taken to address the breach; and</li> <li>• any steps they can take to protect themselves from harm.</li> </ul>	<p><a href="#">Breach reporting   ICO</a></p>
<p>How should a qualified trust service provider verify the identity of its customers?</p>	<ul style="list-style-type: none"> <li>• If you are a qualified trust service provider, UK eIDAS Regulation Article 24(1) requires you to verify the identity of any individual or organisation to whom you issue a qualified certificate. It sets out four verification options:</li> <li>• in person, by the physical presence of the person or authorised representative of the organisation;</li> <li>• using electronic ID that was itself originally verified in person, and meets the eIDAS assurance level of "substantial" or "high" set out in EU eIDAS Regulation Article 8;</li> <li>• using a certificate of a qualified electronic signature or seal that was itself verified in person or using electronic ID as set out above; or</li> <li>• using another method recognised by the UK government which is confirmed by a conformity assessment body as being as reliable as verification in person. If you choose this option</li> </ul>	<p><a href="#">Qualified trust service provider obligations   ICO</a></p>



	<p>you will need to provide evidence that this is the case.</p> <ul style="list-style-type: none"> <li>You can carry the verification out yourself or use a subcontractor.</li> </ul>	
What should be included in a 'qualified certificate database'?	It's up to you to decide exactly what details you include, but as a minimum it should show the status of each certificate – that is, whether it is valid, suspended, expired or revoked. You will therefore need to include a certificate's issue date, expiry date, and any revocation date.	<a href="#">Qualified trust service provider obligations   ICO</a>
How long does a qualified trust service provider have to remove a revoked certificate off their database?	As soon as possible and within 24 hours	<a href="#">Qualified trust service provider obligations   ICO</a>
Does a qualified trust service provider need liability insurance?	The Regulation requires you to either maintain sufficient funds to cover any legal claims, or obtain appropriate insurance cover for this risk.	<a href="#">Qualified trust service provider obligations   ICO</a>
What is a 'termination plan'?	You need to create a plan to deal with the issues that will arise if and when you decide to stop providing a qualified trust service. In particular, the plan needs to set out what records you will keep after termination to provide continuity of service and to provide evidence in court if necessary. You also need to include how long this information will be retained for. You must keep the plan updated.	<a href="#">Qualified trust service provider obligations   ICO</a>
How does a provider maintain qualified status?	To maintain qualified status you will need to undergo the conformity assessment process every two years, at your own expense.	<a href="#">Becoming a qualified trust service provider   ICO</a>
What tools does the ICO have for taking	We can:	<a href="#">Enforcement   ICO</a>

<p>action to enforce eIDAS?</p>	<ul style="list-style-type: none"> <li>• conduct an audit to check you are complying with your obligations as a trust service provider, and make recommendations;</li> <li>• serve an Enforcement Notice order if there has been a breach, requiring an organisation to take specified steps to comply with the law;</li> <li>• issue a Monetary Penalty Notice requiring you to pay £1,000;</li> <li>• prosecute you if you fail to comply with an Enforcement Notice (except in Scotland, where the Procurator Fiscal brings prosecutions); an</li> <li>• report to Parliament on issues of concern.</li> </ul>	
<p>What happens if an organisation fails to comply with an ICO enforcement notice?</p>	<p>The ICO has the power to impose more substantial fines of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.</p>	<p><a href="#">Enforcement   ICO</a></p>

## Case Study 1

### Points to include in your response:

Individuals can make a **subject access request** to the organisation to request a copy of any personal data held about them.

Individuals have a right to rectification - Organisations have an obligation to ensure that personal data is **factually accurate**.

**Opinions** provided about an individual are not generally considered to be factual information.

**Raising a concern** with the organisation. Not necessary to include HTC to ICO but should explain our role.

### Useful Links

Your right to access your personal data (subject access)

<https://ico.org.uk/your-data-matters/your-right-of-access/>

Your right to have your data corrected

<https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected/>

Raise a concern with an organisation:

<https://ico.org.uk/your-data-matters/raising-concerns/>

Detailed guidance on employment practices

[https://ico.org.uk/media/for-organisations/documents/1064/the\\_employment\\_practices\\_code.pdf](https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf)

## Case Study 2

### Notes

Data protection legislation **does not prevent** individuals from installing CCTV on their domestic property.

Explain what the ICO can/cannot do in relation to domestic CCTV and how to raise a concern.

Explain difference in cameras that capture images inside/outside property boundaries:

- If CCTV is installed in a way that it **does not capture** images outside of the boundary of a private property, the images captured via the CCTV will be **exempt from data protection legislation**. This is because the legislation **does not** relate to personal information that is processed for purely personal or household activity.
- When CCTV **captures images outside the boundary** of a private property, the operator of the CCTV will **have to comply** with the data protection obligations.

**DP obligations** - Signage, retention and subject access requests, for example, apply to the CCTV images (Remember, there's no longer a need to register domestic CCTV with the ICO)

**Harassment** - Referral to the Police regarding any harassment concerns.

### Useful links

Guidance for people being filmed

<https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-being-filmed/>

Tool for identifying best course of action

<https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-being-filmed/i-m-unhappy-about-the-use-of-a-home-cctv-system-what-can-i-do/>

## Case Study – Notes

### Notes

Individuals can make a **subject access request** to the organisation to request a copy of any personal data held about them. Organisations must respond to a Subject Access Request (SAR) within one month.

### Things to consider

It would be worth explaining the rules around the deadlines for a subject access request.

One month has passed but no response whatsoever has been provided. It is not clear whether the individual has chased their request in writing and they have been unable to contact them via phone.

We would need to advise them to contact the organisation, raising a concern. They may have already done this, so we would also explain how to bring a complaint to ourselves.

### Useful Links

Your right to access your personal data (subject access)  
<https://ico.org.uk/your-data-matters/your-right-of-access/>

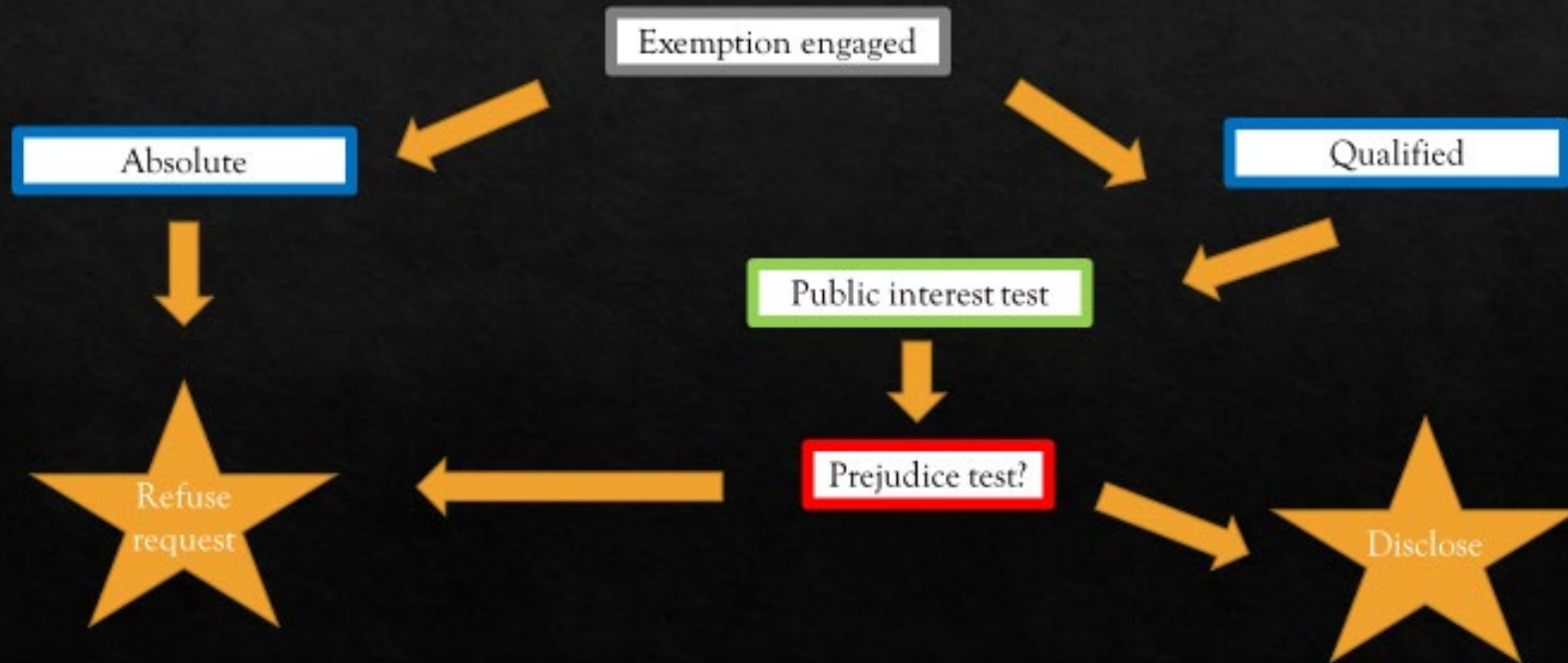
Raise a concern with an organisation:  
<https://ico.org.uk/your-data-matters/raising-concerns/>

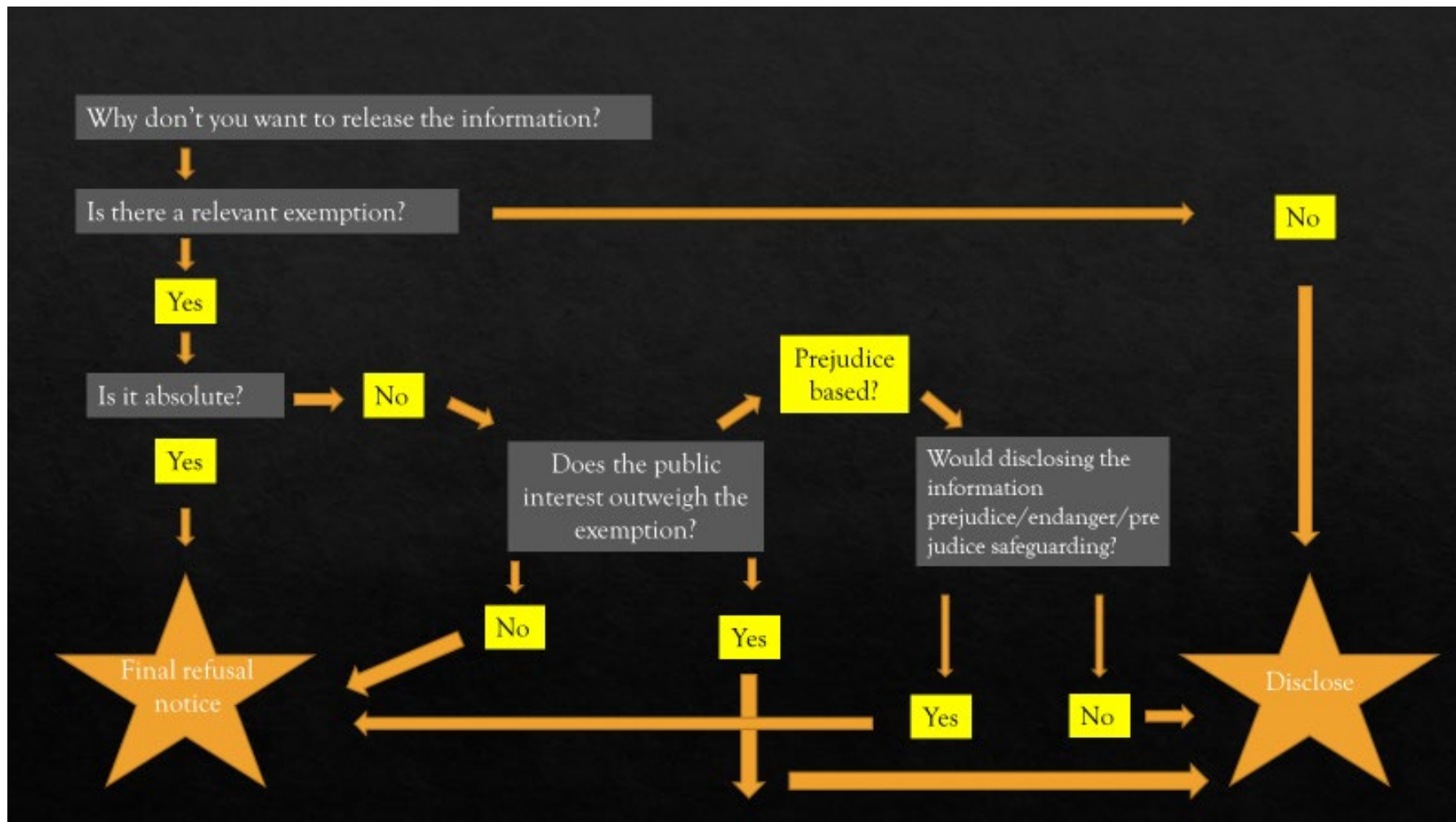
Making a complaint:  
<https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>

# Absolute and qualified exemptions

Exempt means falls within / engages an exemption

However, it may still be disclosable if its within the public interest.





## The Freedom of Information Act quiz

The aim of this quiz is to help staff understand the FOI Act. All the answers to these questions can be found on our website. Staff can point customers to these areas when they are in contact with them.

Question	Answer	Source
What are the 2 main obligations of a public authority under FOIA	<ol style="list-style-type: none"><li>1. Proactively publish information.</li><li>2. Respond to information requests</li></ol>	<a href="#">Public authority obligations</a>
Who can amend Schedule 1?	Chancellor of the Duchy of Lancaster	<a href="#">Amending schedule 1</a>
Which Government department updates Schedule 1?	Cabinet Office	<a href="#">Government department - schedule 1 or Public authorities under the Freedom of Information Act   ICO</a>
What does wholly owned by the Crown mean? Give an example of such a company	Any company wholly owned by a government department eg Northern Ireland Water, UK Financial Investments Ltd or Commonwealth Development Corporation	<a href="#">Wholly owned by the Crown</a>
Where does the term wider public sector come from?	Protection of Freedoms Act 2012	<a href="#">Public sector</a>



<p>What does wholly owned by a wider public sector mean? Give an example.</p>	<p>A company owned by a relevant PA in schedule 1 (not government department or an authority listed only in relation to particular information e.g. BBC) and every member is a relevant PA – therefore it can be owned by more than relevant PA.</p>	<p><a href="#">Wholly owned by a wider public sector</a></p>
<p>What is derogated information? Give examples of 2 PA's this applies to</p>	<p>Information that is held by a PA but is not subject to FOIA. BBC, CMA, UCAS, GP's Practices</p>	<p><a href="#">Derogated information</a></p>
<p>Can information held in a private email account of a Councillor be subject to FOIA?</p>	<p>Yes – if it relates to the business of the Council</p>	<p><a href="#">Official information held in non-corporate communications channels   ICO</a></p>
<p>Where can you find guidance on when information is held on behalf of another person?</p>	<p>Information held by a public authority for the purposes of the Freedom of Information Act</p>	<p><a href="#">Information held on behalf of another person</a></p>
<p>Give examples of the types of documents covered by FOIA</p>		<p><a href="#">Documents covered by FOIA</a></p>

Give examples of what recorded information may cover in terms of a document	Design and layout Logos and letterheads Language Emphasised wording Handwriting Annotations, headers and footers Images Email transmission data	<a href="#">The right to recorded information and requests for documents   ICO</a>
List 3 risks created by poor records management		<a href="#">section-46-code-of-practice-records-management-foia-and-eir.pdf (ico.org.uk)</a>
List 3 reasons records can be kept for longer than the PA needs them for		<a href="#">section-46-code-of-practice-records-management-foia-and-eir.pdf (ico.org.uk)</a>
Is it possible to commit a criminal offence under FOI?	Yes – section 77	

## The Freedom of Information Act quiz – Part 2

The aim of this quiz is to help staff understand the FOI Act. All the answers to these questions can be found on our website. Staff can point customers to these areas when they are in contact with them.

Question	Answer	Source
List 3 benefits of conforming to the Request handling Code of Practice		<a href="#">Section 45 – Code of Practice, request handling   ICO</a>
What should PA's include in their procedures for dealing with requests and where is this outlined?	<p>Website guidance states:</p> <ul style="list-style-type: none"> <li>• a contact address. That is, a postal and email address or an appropriate online alternative such as an online form;</li> <li>• a telephone number;</li> <li>• ideally, a named individual to help applicants direct their requests for information or assistance.</li> </ul>	<p><a href="#">Dealing with request procedures</a> THIS LINKS TO 2004 VERSION OF CODE.</p> <p>2018 VERSION LINK FOUND HERE: <a href="#">Section 45 – Code of Practice, request handling   ICO</a></p> <p>BUT GUIDANCE HERE MIGHT BE BETTER FOR BAS STAFF: <a href="#">Section 16 – Advice and Assistance   ICO</a></p>
What must be included in a request for information?	Real name Address for correspondence	<a href="#">Valid requests</a>

	Description of information required	
What are the options when a request is received for information held on behalf of another PA?	<ol style="list-style-type: none"> <li>1. Redirect the requester.</li> <li>2. Transfer the request to the originating PA.</li> <li>3. Deal with the request but consult with the originating PA on disclosure decision (?).</li> </ol> <p>DO 2 AND 3 STILL APPLY? WEBSITE GUIDANCE OPPOSITE MAKES NO MENTION OF THESE, ONLY 1.</p>	<a href="#">Information held on behalf of another PA</a> OUT-OF-DATE LINK  <a href="#">Information you hold for the purposes of FOIA   ICO</a>
How should a conditional request be handled where a change is anticipated?	Asked to resubmit when condition is satisfied	<a href="#">Conditional requests</a>
Are requests for schedules and lists considered to be creating new information if not held in that format?		<a href="#">Determining whether we hold information   ICO</a>
How long does a state maintained school have to respond to an FOI request?	20 school days or 60 working days	<a href="#">State and maintained schools</a>

What should be considered when dealing with a 'round robin' requests and whether it is vexatious?

[Are round robin requests vexatious? | ICO](#)

### The Freedom of Information Act quiz – Part 3

The aim of this quiz is to help staff understand the FOI Act. All the answers to these questions can be found on our website. Staff can point customers to these areas when they are in contact with them.

Question	Answer	Source
What must be included in a refusal notice?		<a href="#">Refusal notices</a>
List 3 possible benefits to issuing a well written refusal notice		<a href="#">refusing a request writing a refusal notice foi.pdf (ico.org.uk) – Page 12</a> <a href="#">Refusing a request: writing a refusal notice (section 17)   ICO</a>
Which exemption does not include the provision that removes the duty to confirm or deny whether information is held?	Section 21	<a href="#">When to refuse to confirm or deny information is held</a> Link says "page not found".  Correct link is: <a href="#">Information reasonably accessible to the applicant by other means (section 21) (ico.org.uk)</a> Para 9.
What are the 3 steps to the prejudice test?	1. Identify applicable interests 2. Identify the nature of the prejudice 3. Decide on likelihood of the occurrence of prejudice	<a href="#">Prejudice tests</a>  <a href="#">3 step test</a>

Which hold the greater possibility of prejudice 'would' or 'would be likely to'	Would	<a href="#">Prejudice possibility</a>
What is meant by an absolute exemption and provide an example?	No requirement to apply the PIT S21,23,32,34,36,40(1)(2),41 &44	<a href="#">Absolute exemption</a> Or: <a href="#">When can we refuse a request for information?   ICO</a>
What is meant by a class based exemption?	Means that if the information is of the type described in the exemption, then it is covered by that exemption.	<a href="#">Class based exemption</a>
How long can the time to respond to a request be extended by when applying the public interest test?	20 working days in most cases, anything longer would be exceptional.	<a href="#">Time limits for compliance under the Freedom of Information Act (Section 10)   ICO</a>
What do the PA have to do if they decide to claim the extra time?	To claim this extra time, you must: <ul style="list-style-type: none"> <li>• contact the requester in writing within the standard time for compliance;</li> </ul>	<a href="#">Claiming extra time to respond</a> Better link is: <a href="#">Time limits for compliance under the Freedom of Information Act (Section 10)   ICO</a>

	<ul style="list-style-type: none"><li>• specify which exemption(s) you are seeking to rely on; and</li><li>• give an estimate of when you will have completed the public interest test.</li></ul>	
--	---	--



## **Freedom of Information /Environmental Information Regulations**

### What is the Freedom of Information Act?

The Freedom of Information Act 2000 provides public access to recorded information held by public authorities. The Act covers all recorded information held by a public authority. So it is not limited to official documents. It covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings. It is also not limited to information created by the public authority, so it also covers, for example, letters received from members of the public, information supplied by third party companies, although there may be a good reason not to release them.

Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason and it is permitted by the Act

The Act only covers public authorities. Schedule 1 of the Act contains a list of the bodies that are classed as public authorities in this context. Some of these bodies are listed by name, such as the Health and Safety Executive or the National Gallery. Others are listed by type, for example government departments, parish councils, or maintained schools.

### What is a publication scheme?

Public authorities are obligated to publish certain information. Every public authority are required to have a publication scheme which is approved by the ICO and to publish the information that is covered by the scheme proactively. To help, the ICO has developed a model publication scheme.

The scheme must set out their commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information.

The information provided in a publication scheme represents the minimum a public authority must disclose. If a member of the public wants information not listed in the scheme, they can still ask for it.

### What is EIR?

The Environmental Information Regulations 2004 are derived from European law, and provide public access to environmental information held by public authorities plus some others eg water companies and power companies as these have an impact on the environment. The Regulations apply only to the environmental information held by public authorities/private companies caught by the scope of the regulations.

The Regulations give people a right of access to information about the activities of public authorities that relate to or affect the environment, unless there is good reason for them not to have the information. This is sometimes referred to as a presumption in favor of disclosure.

The EIR also requires any body covered by the act to produce a publication scheme in relation to the environmental information they hold. The Regulations require them to do this in the following two ways:

- The published information should be in easily accessible electronic means; and
- The records should be organised in such a way that they can publish certain information routinely.

They don't have to publish all the environmental information they hold. The minimum they should routinely publish to comply with their obligations under the Regulations includes things like policies, plans and procedures relating to the environment, reports on the state of the environment, and environmental impact studies. It also includes data taken from monitoring activities and risk assessments that affect or are likely to affect the environment.

#### What is a valid request?

For FOI a request should be made in writing however EIR allows verbal requests to be made. **\*click\***

Requesters do not have to mention the Act or direct their request to a designated member of staff.

This doesn't mean that a public authority has to treat every enquiry formally as a request under the Act. It will often be most sensible and provide better customer service to deal with it as a normal customer enquiry under their usual customer service procedures, for example, if a member of the public wants to know what date their rubbish will be collected, or whether a school has a space for their child.

There will be occasions where a request is made under the Act but does not in fact meet the above description of being a request for recorded information. This may include requests for explanations, clarification of policy, comments on the public authority's business, and any other correspondence that does not follow the definition of a valid request.

The provisions of the Act will to come into force only if:

The public authority cannot provide the requested information straight away; or  
the requester makes it clear they expect a response under the Act.

The request could be a letter or email. And they can also be made via the web, or even on social networking sites such as Facebook or Twitter if the public authority uses these.

**\*click\***

- It should include the name of the requester.  
**\*click\***
- It should include an address for correspondence.  
**\*click\***
- It should describe the information being requested.

Can a charge be made for information?

**FOI**

The FOIA allows the public authority to charge for providing information in a publication scheme (s19(2)).

A public authority can recover their communication costs, such as for photocopying, printing and postage. However, they cannot normally charge for any other costs, such as for staff time spent searching for information, unless other relevant legislation authorises this. There is no maximum or minimum cost limit, but any charges made must be reasonable and justifiable. If they wish to charge a fee, they should send the requester a fees notice.

This is different to Section 12 of FOIA, where a request can be refused or charged for if the cost of compliance to the right of access exceeds the appropriate limit. A fee can be charged based on the number of hours spent determining if the information is held, locating it, retrieving it and extracting the relevant information.

In relation to cost Limits - staff time is charged at £25 per person per hour, regardless of who does the work, including external contractors. This means a limit of 18 or 24 staff hours, depending on whether the £450 or £600 limit applies to the public authority. The £600 limit only applies to central government organisations, all other public authorities will fall into the £450 cost limit.

They cannot take into account the time they are likely to need to decide whether exemptions apply, to redact (edit out) exempt information, or to carry out the public interest test.

It is not possible to charge for any staff time where the cost of compliance falls below the cost limit. There is no obligation to comply with any

request exceeding the cost limit. However, should a public authority decide to respond to a request that exceeds the cost limit on a voluntary basis it can charge for the staff time needed to do so.

In such circumstances staff time is chargeable at a standard rate, including the cost of making redactions (but only the physical cost of making redactions and not staff time for considering whether exemptions apply), to be included in the initial fees notice.

**\*click\***

### **EIR**

In some circumstances EIR allows a fee for making the information available. Any charge should be 'reasonable' – it should not exceed the costs incurred in making the information available or act as a deterrent to the right to request information.

It may cover the cost of the paper for photocopying, printing the information, a covering letter and the cost of postage. It may also include the cost of staff time in identifying, locating or retrieving the information from storage.

If a fee is being charged, the requester should be referred to the schedule of charges within 20 working days. If they need to pay in advance, they should tell the requester this, and the amount. The information does not have to be provided until the fee is received.

How long does a PA have to respond?

**\*click\***

### **FOI.**

They have 20 working days to respond. For schools, the standard time limit is 20 school days, or 60 working days if this is shorter.

If they wish to charge a fee, they should send the requester a fees notice. They do not have to send the information until they have received the fee. The time limit for complying with the request excludes the time spent waiting for the fee to be paid. In other words, they should issue the fees notice within the standard time for compliance. Once they have received the fee, they should send out the information within the time remaining. We call this "stopping the clock".

**\*click\***

### **EIR**

The Regulations say information should be made available as soon as possible, and no later than 20 working days. The first working day after a request is received is the first day. Working day means any day other than a Saturday, Sunday, or public holidays and bank holidays; this may

or may not be the same as the days an organisation are open for business or staff are in work.

### Can a request for information be refused?

#### **FOI**

The Freedom of Information Act contains a number of exemptions that allow a public authority to withhold information from a requester. In some cases it will allow them to refuse to confirm or deny whether they hold information.

Some exemptions relate to a particular type of information, for instance, information relating to government policy, these are called class based exemptions. Other exemptions are based on the consequences that would arise or would likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests. These are called prejudice based.

There is also an exemption for personal data if releasing it would be contrary to the Data Protection Act.

A public authority can automatically withhold information because an exemption applies, and that exemption is 'absolute'. All absolute exemptions are class based. However, most exemptions are not absolute but require a public interest test to be applied, these are qualified exemptions. This means the public interest arguments must be considered before deciding whether to disclose the information. So information may have to be disclosed in spite of an exemption, where it is in the public interest to do so.

#### **EIR**

The Environmental Information Regulations state exceptions that allow information requests to be refused. Some of the exceptions relate to categories of information, for example, unfinished documents and internal communications. Others are based on the harm that would arise from disclosure, for example, if releasing the information would adversely affect international relations or intellectual property rights, however some of the exceptions do not apply to information about emissions.

There is also an exception for personal data if providing it would be contrary to the Data Protection Act.

Under the Regulations, most exceptions are subject to the public interest test. This is an extra stage in the process of deciding what information to provide, which requires the balancing of the public interest arguments for disclosing the information against those for upholding the exception. This means that even if disclosing information would harm, for example, international relations, an organisation must still release the information if

the public interest arguments for disclosing it are stronger. The public interest is not necessarily the same as what the public finds interesting.

### What should be in a refusal notice?

When refusing all or part of a request, the requester must be sent a written refusal notice. A refusal notice must be issued even when either the public authority are refusing to say whether they hold information at all, or confirming that information is held but refusing to release it.

A refusal notice should;

**\*Click\***

- explain what section of the legislation is being relied on to refuse the request and why;  
**\*Click\***
- give details of any internal review/complaints procedure offered by the organisation or state that they do not have one; and  
**\*Click\***
- explain the requester's right to complain to the ICO, including contact details for this.

### Complaints

The ICO has a general duty to investigate complaints from members of the public who believe that an authority has failed to respond correctly to a request for information. If someone makes a complaint against a public authority, our complaints handling process gives them an opportunity to reconsider their actions and put right any mistakes without us taking any formal action. If the complaint is not resolved informally, we will issue a decision notice. If we find that they have breached the Act, the decision notice will say what they need to do to put things right.

We also have powers to enforce compliance if a public authority has failed to adopt the publication scheme or has not published information as they should, this is despite whether or not we have received a complaint about this.


A public authority may be breaching the Freedom of Information Act if they do any of the following:

- fail to respond adequately to a request for information;
- fail to adopt the model publication scheme, or do not publish the correct information; or
- deliberately destroy, hide or alter requested information to prevent it being released.

This last point is the only criminal offence in the Act that individuals and public authorities can be charged with.

Other breaches of the Act are unlawful but not criminal. The ICO cannot issue a fine if a public authority fails to comply with the Act, nor can we require them to

pay compensation to anyone for breaches of the Act. However, they should correct any mistakes as soon as they are aware of them. Failure to comply with a decision notice however, is contempt of court, punishable by a fine.



Freedom of Information Act  
2000  
Environmental Information  
Regulations 2004



## What is the Freedom of Information Act?

The Act covers all recorded information held by a **public authority**. It provides public access to this information, unless an exemption applies.

**Schedule 1** of the Act contains a list of the bodies that are classed as public authorities in this context

The Freedom of Information Act 2000 provides public access to recorded information held by public authorities. The Act covers all recorded information held by a public authority. So it is not limited to official documents. It covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings. It is also not limited to information created by the public authority, so it also covers, for example, letters received from members of the public, information supplied by third

party companies, although there may be a good reason not to release them.

Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason and it is permitted by the Act

The Act only covers public authorities. Schedule 1 of the Act contains a list of the bodies that are classed as public authorities in this context. Some of these bodies are listed by name, such as the Health and Safety Executive or the National Gallery. Others are listed by type, for example government departments, parish councils, or maintained schools.

## Publication Schemes

- Every public authority are required to have a publication scheme, approved by the Information Commissioner's Office (ICO), and to publish information covered by the scheme.
- The scheme must set out their commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information.

Public authorities are obligated to publish certain information. Every public authority are required to have a publication scheme which is approved by the ICO, and to publish the information that is covered by the scheme. To help, the ICO has developed a model publication scheme proactively.

The scheme must set out their commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information.

The information provided in a publication scheme represents the minimum a public authority must disclose. If a member of the public wants information not listed in the scheme, they can still ask for it.

## What is EIR?

- Environmental Information Regulations 2004 provide public **access to environmental information** held by public authorities plus some others eg water companies
- The Regulations give people a right of access to information about the activities of public authorities that **relate to or affect the environment**

The Environmental Information Regulations 2004 are derived from European law, and provide public access to environmental information held by public authorities plus some others eg water companies and power companies as these have a large impact on the environment. The Regulations apply only to the environmental information held by public authorities/private companies caught within the scope of the regulations.

The Regulations give people a right of access to information about the activities of public authorities that relate to or affect the environment, unless there is good reason for them not to have the information. This is sometimes referred to as a presumption in favour of disclosure.

The EIR also requires any body covered by the act to produce a publication scheme in relation to the environmental information they hold.

The Regulations require them to do this in the following two ways:

- The published information should be in easily accessible electronic means; and
- The records should be organised in such a way that they can publish certain information routinely.

They don't have to publish all the environmental information they hold. The

minimum they should routinely publish to comply with their obligations under the Regulations includes things like policies, plans and procedures relating to the environment, reports on the state of the environment, and environmental impact studies. It also includes data taken from monitoring activities and risk assessments that affect or are likely to affect the environment.

## What is a Valid Request?

For FOIA a request should be made **in writing** however EIR allows **verbal** requests to be made.

It should include the name of the requester.

It should include an address for correspondence.

It should describe the information being requested.

For FOI a request should be made in writing however EIR allows verbal requests to be made. **\*click\***

Requesters do not have to mention the Act or direct their request to a designated member of staff.

This doesn't mean that a public authority has to treat every enquiry formally as a request



under the Act. It will often be most sensible and provide better customer service to deal with it as a normal customer enquiry under their usual customer service procedures, for example, if a member of the public wants to know what date their rubbish will be collected, or whether a school has a space for their child.

There will be occasions where a request is made under the Act but does not in fact meet the above description of being a request for recorded information. This may include requests for explanations, clarification of policy, comments on the public authority's business, and any other correspondence that does not follow the definition of a valid request.

The provisions of the Act will to come into force only if:

The public authority cannot provide the

requested information straight away; or the requester makes it clear they expect a response under the Act.

The request could be a letter or email. And they can also be made via the web, or even on social networking sites such as Facebook or Twitter if the public authority uses these.

- **\*click\***
- It should include the name of the requester.
- **\*click\***
- It should include an address for correspondence.
- **\*click\***
- It should describe the information being requested.

## Charging for Information

The **FOIA** allows the public authority to charge for providing information in a **publication scheme** (s19(2)).

Section 12 puts limitations on the right of access, where a charge can be made if the cost for compliance exceeds the appropriate limit

---

In some circumstances **EIR** allows a fee for making the information available (reg. 8)

The information does not have to be provided until the fee is received.

The FOIA allows the public authority to charge for providing information in a publication scheme (s19(2)). **\*Click\***

A public authority can recover their communication costs, such as for photocopying, printing and postage. However, they cannot normally charge for any other costs, such as for staff time spent searching for information, unless other relevant legislation authorises this. There is no

maximum or minimum cost limit, but any charges made must be reasonable and justifiable. If they wish to charge a fee, they should send the requester a fees notice.

This is different to Section 12 of FOIA, where a request can be refused or charged for if the cost of compliance to the right of access exceeds the appropriate limit. A fee can be charged based on the number of hours spent determining if the information is held, locating it, retrieving it and extracting the relevant information.

In relation to cost Limits - staff time is charged at £25 per person per hour, regardless of who does the work, including external contractors. This means a limit of 18 or 24 staff hours, depending on whether the £450 or £600 limit applies to the public authority. The £600 limit only applies to central government organisations, all other public authorities will fall into the £450 cost limit.

They cannot take into account the time they are likely to need to decide whether exemptions apply, to redact (edit out) exempt information, or to carry out the public interest test.

It is not possible to charge for any staff time where the cost of compliance falls below the cost limit. There is no obligation to comply with any request exceeding the cost limit. However, should a public authority decide to respond to a request that exceeds the cost limit on a voluntary basis it can charge for the staff time needed to do so.

In such circumstances staff time is chargeable at a standard rate, including the cost of making redactions (but only the physical cost of making redactions and not staff time for considering whether exemptions apply), to be included in the initial fees notice.

**\*click\***

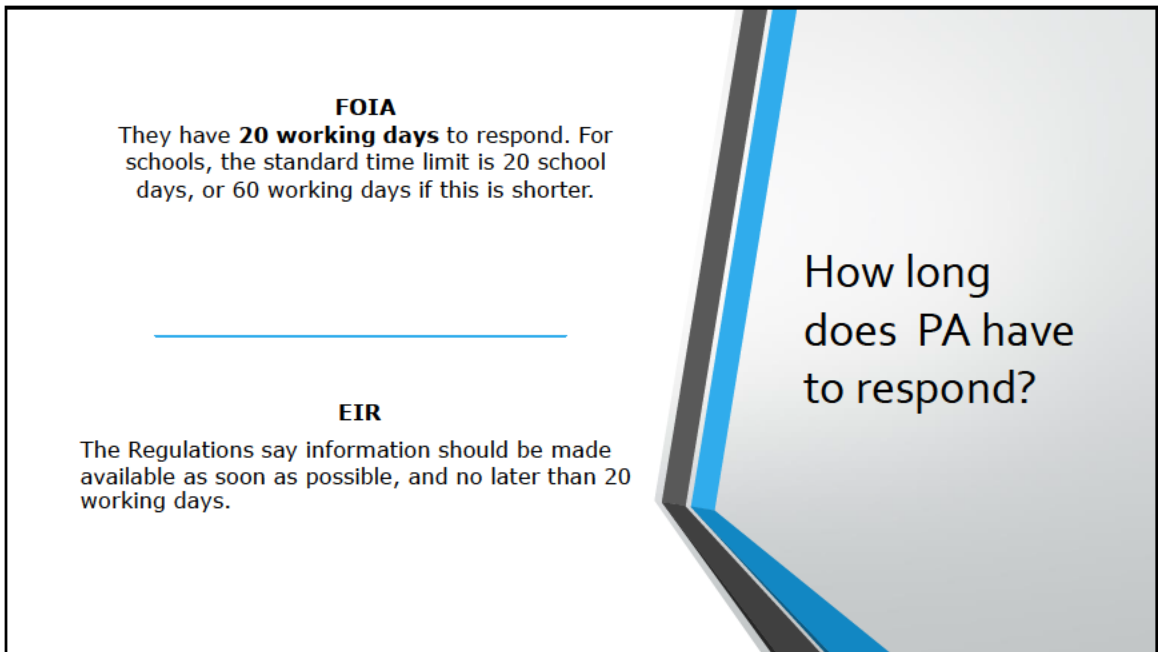
## **EIR**

In some circumstances EIR allows a fee for making the information available. Any charge should be 'reasonable' – it should not exceed the costs incurred in making the information available or act as a deterrent to the right to request information.

It may cover the cost of the paper for photocopying, printing the information, a covering letter and the cost of postage. It may also include the cost of staff time in identifying, locating or retrieving the information from storage.

If a fee is being charged, the requester should be referred to the schedule of charges within 20 working days. If they need to pay in advance, they should tell the requester this, and the amount. The information does not have to be provided until the fee is

received.



**\*click\***

## **FOI.**

They have 20 working days to respond. For schools, the standard time limit is 20 school days, or 60 working days if this is shorter.

If they wish to charge a fee, they should send the requester a fees notice. They do not have to send the information until they have received the fee. The time limit for complying



with the request excludes the time spent waiting for the fee to be paid. In other words, they should issue the fees notice within the standard time for compliance. Once they have received the fee, they should send out the information within the time remaining. We call this "stopping the clock".

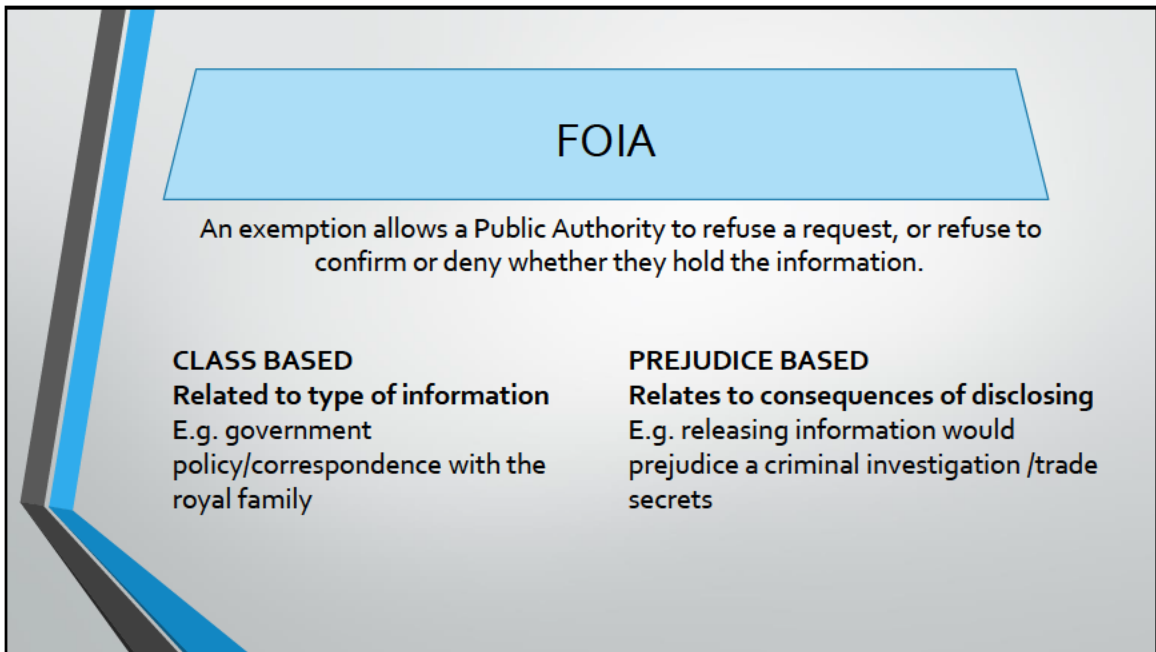
**\*click\***

## **EIR**

The Regulations say information should be made available as soon as possible, and no later than 20 working days. The first working day after a request is received is the first day. Working day means any day other than a Saturday, Sunday, or public holidays and bank holidays; this may or may not be the same as the days an organisation are open for business or staff are in work.

Can a request  
for information  
be refused?



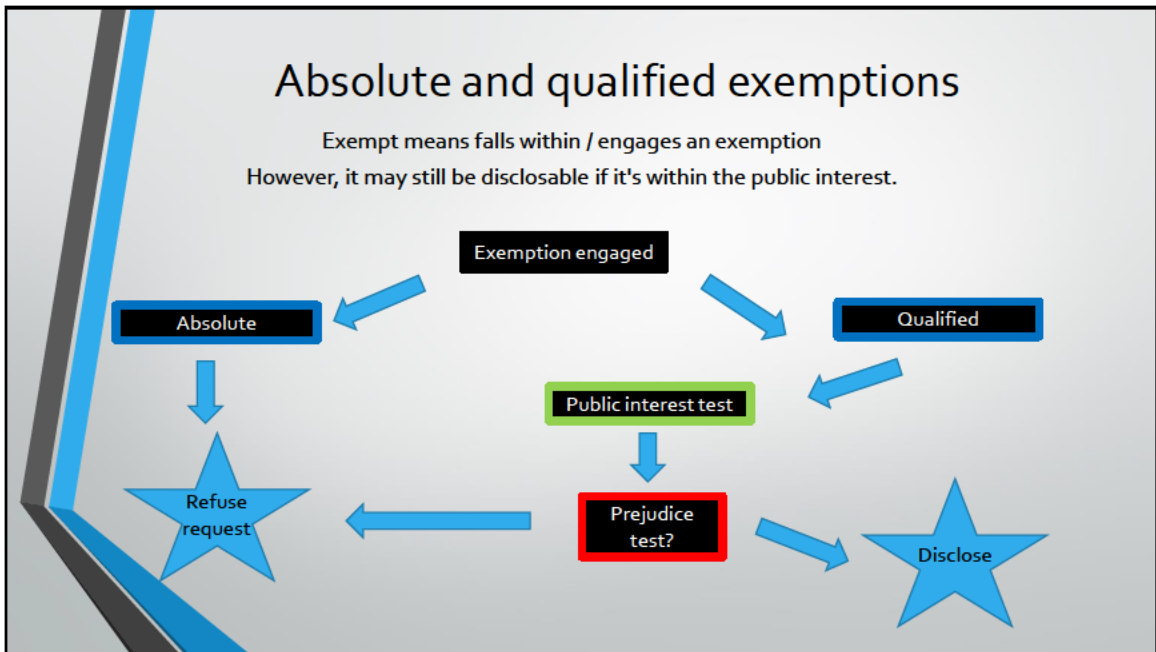


The Freedom of Information Act contains a number of exemptions that allow a public authority to withhold information from a requester. In some cases it will allow them to refuse to confirm or deny whether they hold information.

Some exemptions relate to a particular type of information, for instance, information relating to government policy, these are called class based exemptions. Other

exemptions are based on the consequences that would arise or would likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests. These are called prejudice based.

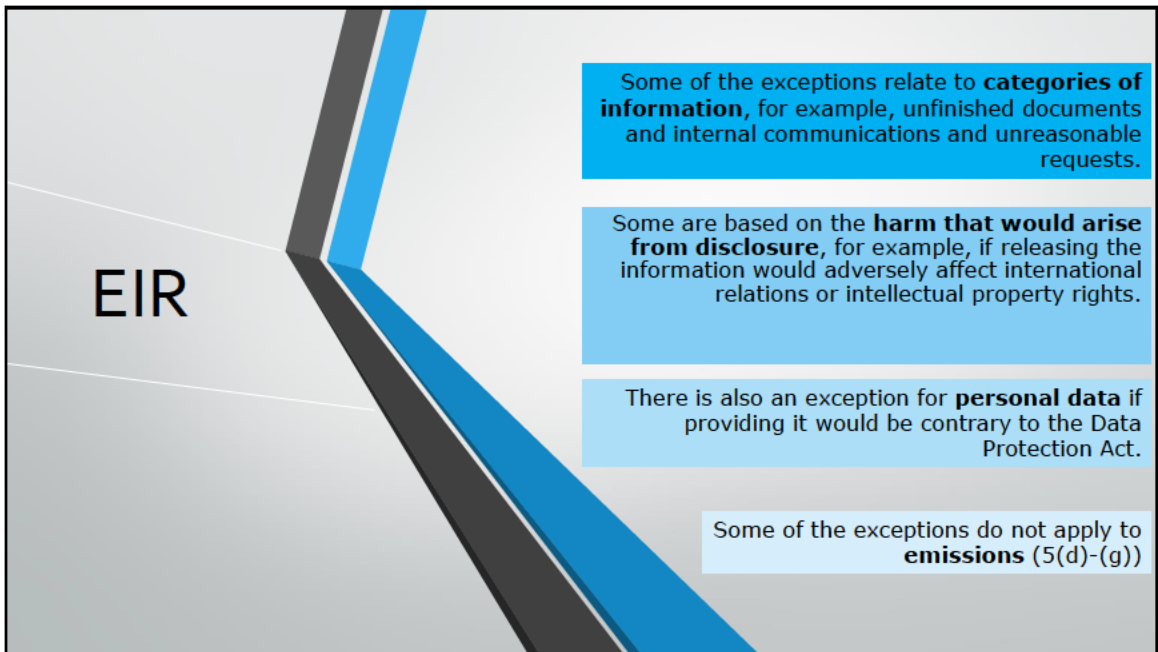
There is also an exemption for personal data if releasing it would be contrary to the Data Protection Act.



A public authority can automatically withhold information because an exemption applies, and that exemption is 'absolute'. All absolute exemptions are class based. However, most exemptions are not absolute but require a public interest test to be applied, these are qualified exemptions. This means the public interest arguments must be considered before deciding whether to disclose the information. So information may have to be disclosed in spite of an exemption, where it is

in the public interest to do so.

Explain diagram



## **EIR**

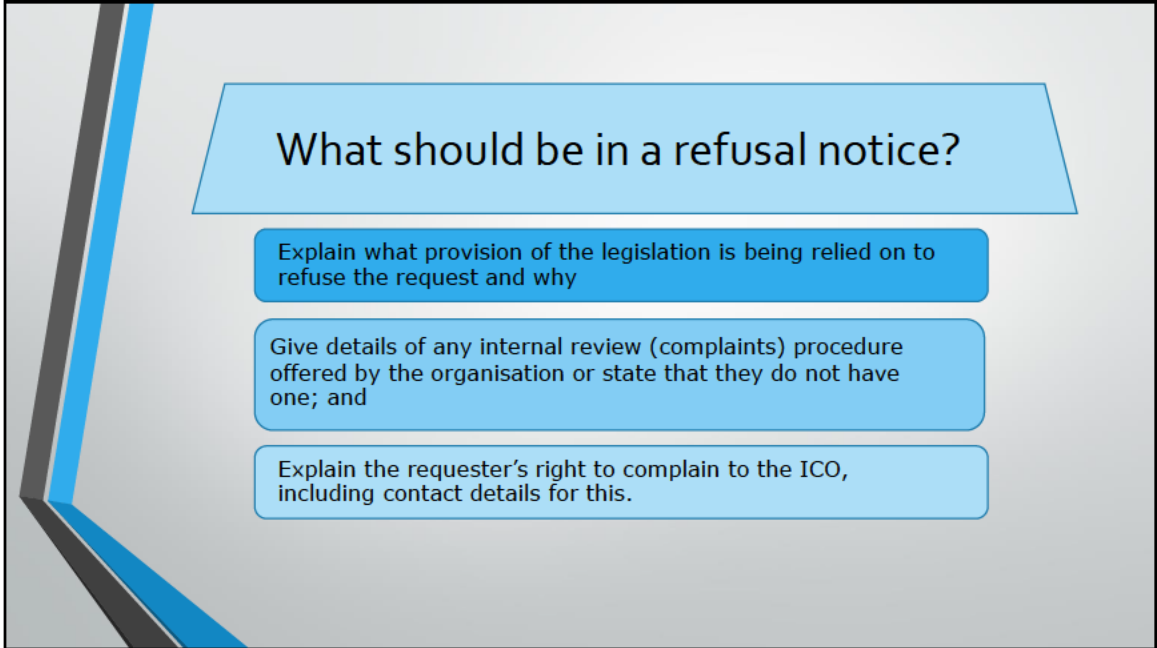
The Environmental Information Regulations state exceptions that allow information requests to be refused. Some of the exceptions relate to categories of information, for example, unfinished documents and internal communications. Others are based on the harm that would arise from disclosure, for example, if releasing the information would adversely

affect international relations or intellectual property rights, however some of the exceptions do not apply to information about emissions.

There is also an exception for personal data if providing it would be contrary to the Data Protection Act.

Under the Regulations, most exceptions are subject to the public interest test. This is an extra stage in the process of deciding what information to provide, which requires the balancing of the public interest arguments for disclosing the information against those for upholding the exception. This means that even if disclosing information would harm, for example, international relations, an organisation must still release the information if the public interest arguments for disclosing it are stronger. The public interest is not necessarily the same as what the public finds interesting.



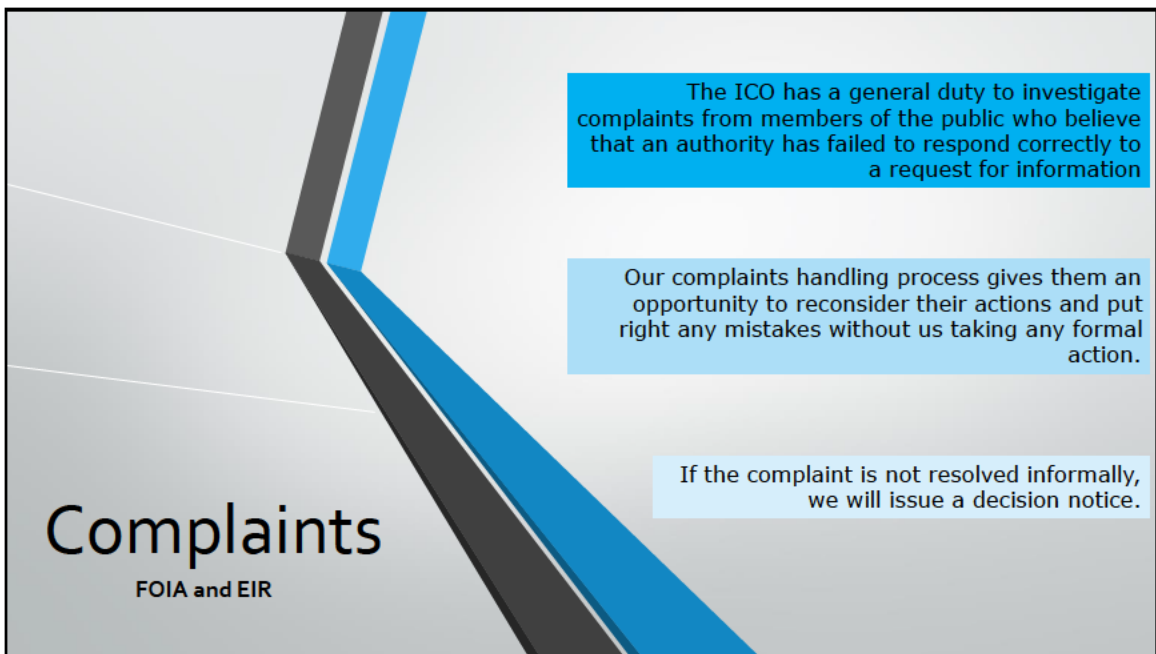


When refusing all or part of a request, the requester must be sent a written refusal notice. A refusal notice must be issued even when either the public authority are refusing to say whether they hold information at all, or confirming that information is held but refusing to release it.

A refusal notice should;

**\*Click\***

- explain what section of the legislation is being relied on to refuse the request and why;  
**\*Click\***
- give details of any internal review/ complaints procedure offered by the organisation or state that they do not have one; and  
**\*Click\***
- explain the requester's right to complain to the ICO, including contact details for this.



The ICO has a general duty to investigate complaints from members of the public who believe that an authority has failed to respond correctly to a request for information. If someone makes a complaint against a public authority, our complaints handling process gives them an opportunity to reconsider their actions and put right any mistakes without us taking any formal action.

If the complaint is not resolved informally, we

will issue a decision notice. If we find that they have breached the Act, the decision notice will say what they need to do to put things right.

We also have powers to enforce compliance if a public authority has failed to adopt the publication scheme or has not published information as they should, this is despite whether or not we have received a complaint about this.

A public authority may be breaching the Freedom of Information Act if they do any of the following:

- fail to respond adequately to a request for information;
- fail to adopt the model publication scheme, or do not publish the correct information; or
- deliberately destroy, hide or alter requested information to prevent it being released.

This last point is the only criminal offence in the Act that individuals and public authorities can be charged with.

Other breaches of the Act are unlawful but not criminal. The ICO cannot issue a fine if a public authority fails to comply with the Act, nor can we require them to pay compensation to anyone for breaches of the Act. However, they should correct any mistakes as soon as they are aware of them.

Failure to comply with a decision notice however, is contempt of court, punishable by a fine.

Questions?





Define a data processor (modules 1 & 2 quiz)	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller	<b>Article 4(8) UK GDPR</b>
Define a data subject (modules 1 & 2 quiz)	See the definition of personal data  The identified or identifiable living individual to whom personal data relates	<b>Article 4(1) UK GDPR</b>  <b>Section 3(5)DPA 2018</b>
Does GDPR apply to personal/domestic processing? (modules 1 & 2 quiz)	This Regulation does not apply to the processing of personal data:  (a) by a natural person in the course of a purely personal or household activity	<b>Article 2(2)(a) UK GDPR</b>
Which countries could the UK GDPR apply in? (modules 1 & 2 quiz)	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.  2. This Regulation applies to the processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to:	<b>Article 3 UK GDPR</b>



	<p>(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom; or</p> <p>(b) the monitoring of their behaviour as far as their behaviour takes place within the United Kingdom.</p> <p>3. This Regulation applies to the processing of personal data by a controller not established in the United Kingdom, but in a place where domestic law applies by virtue of public international law</p>	
<p>Explain the principle of transparency  <b>Module 3 question sheet</b>  <b>- Principles 1 – lawful processing</b></p>	<p>The controller shall take appropriate measures to provide any information referred to in <a href="#">Articles 13</a> and 14 and any communication under <a href="#">Articles 15</a> to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.</p> <p>It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.</p> <p>The principle of transparency requires that any information and communication relating to the processing of those personal data be easily</p>	<p><b>Article 12 (1) UK GDPR</b></p> <p><b>Recital 39 UK GDPR</b></p>

	accessible and easy to understand, and that clear and plain language be used	
Explain all six lawful bases for processing (one sentence each) <b>Module 3 question sheet - Principles 1 – lawful processing</b>	Consent Contract Legal obligation Vital interests Public interests Legitimate interests	<b>Article 6 (1) UK GDPR</b>
Define accuracy in data protection terms <b>Module 4 question sheet - Principles 2 – purpose limitation</b>	Accurate and, where necessary, kept up to date; <b>every reasonable step must be taken</b> to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay  The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.  “Inaccurate”, in relation to personal data, means incorrect or misleading as to any matter of fact	<b>Article 5(1)(d) UK GDPR</b>  <b>Article 16 UK GDPR</b>  <b>Section 205 DPA 2018</b>
How long should personal data be retained? <b>Module 4 question sheet</b>	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are	<b>Article 5(1)(e) UK GDPR</b>

<p><b>- Principles 2 – purpose limitation</b></p>	<p>processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with <a href="#">Article 89</a>(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');</p>	
<p>What is data minimisation and why is it important?  <b>Module 4 question sheet - Principles 2 – purpose limitation</b></p>	<p>adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').</p> <p>The controller shall implement appropriate technical and organisational measures for ensuring that, <b>by default</b>, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p>	<p><b>Article 5(1)(c) UK GDPR</b></p> <p><b>Article 25(2) UK GDPR</b></p>
<p>What is the accountability principle?</p>	<p>The controller shall be responsible for, and be <b>able to demonstrate</b> compliance</p>	<p><b>Article 5(2) UK GDPR</b></p>

<p><b>Module 5 question sheet - Principles 3 – security</b></p>	<p>Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able <b>to demonstrate that processing is performed in accordance with this Regulation</b>. Those measures shall be reviewed and updated where necessary.</p>	<p><b>Article 24(1) UK GDPR</b></p>
<p>When must you report a personal data breach? <b>Module 5 question sheet - Principles 3 – security</b></p>	<p>In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.</p>	<p><b>Article 33(1) UK GDPR</b></p>
<p>When must you inform data subjects about a personal data breach? <b>Module 5 question sheet - Principles 3 – security</b></p>	<p>When the personal data breach <b>is likely to result in a high risk</b> to the rights and freedoms of natural persons, the controller shall <b>communicate</b> the personal data breach to the data subject without undue delay.</p>	<p><b>Article 34(1) UK GDPR</b></p>

<p>What is the function of a DPIA?</p> <p><b>Module 5 question sheet - Principles 3 – security</b></p>	<p>Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is <b>likely to result in a high risk</b> to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an <b>assessment of the impact</b> of the envisaged processing operations on the protection of personal data.</p>	<p><b>Article 35(1) UK GDPR</b></p>
<p>What is a subject access request?</p> <p><b>Module 6 question sheet - Individual rights – part 1</b></p>	<p>The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, <b>access</b> to the personal data</p>	<p><b>Article 15(1) UK GDPR</b></p>
<p>Why is the ability to use an access request important to a data subject?</p> <p><b>Module 6 question sheet - Individual rights – part 1</b></p>	<p>A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.</p>	<p><b>Recital 63 UK GDPR</b></p>
<p>How do you exercise your rights?</p> <p><b>Module 6 question sheet - Individual rights – part 1</b></p>	<p>The controller shall facilitate the exercise of data subject rights under <a href="#">Articles 15</a> to 22. In the cases referred to in <a href="#">Article 11(2)</a>, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under <a href="#">Articles 15</a> to 22, unless the controller demonstrates that it is not in a position to identify the data subject.</p>	<p><b>Article 12(2) UK GDPR</b></p>

	<b>Note:</b> GDPR is silent on how an individual exercises their rights – this means any method is appropriate including verbal requests.	
<p>What is the right to be informed about? And how does it work?</p> <p><b>Module 6 question sheet - Individual rights – part 1</b></p>	<p>Personal data shall be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')</p> <p>Information to be provided where personal data are collected from the data subject – <b>to be given at the time of collection</b></p> <p>Information to be provided where personal data have not been obtained from the data subject – <b>to be given within a reasonable period after obtaining the personal data, but at the latest within one month</b></p>	<p><b>Article 5(1)(a) UK GDPR</b></p> <p><b>Article 13 UK GDPR</b></p> <p><b>Article 14 UK GDPR</b></p>
<p>How can an individual complain?</p> <p><b>Module 6 question sheet - Individual rights – part 1</b></p>	<p>Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Commissioner if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.</p>	<p><b>Article 77(1) UK GDPR</b></p>
<p>What is the other name for the right of erasure?</p>	<p>Right to be forgotten</p>	<p><b>Article 17 UK GDPR</b></p>

<b>Module 7 question sheet - Individual rights – part 2</b>		
<p>How could personal data be rectified?</p> <b>Module 7 question sheet - Individual rights – part 2</b>	<p>The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.</p>	<b>Article 16 UK GDPR</b>
<p>When would you use the right to object?</p> <b>Module 7 question sheet - Individual rights – part 2</b>	<p><b>Absolute right:</b></p> <ul style="list-style-type: none"> <li>• direct marketing purposes</li> </ul> <p><b>Qualified right:</b></p> <ul style="list-style-type: none"> <li>• the use of information society services</li> <li>• for scientific or historical research purposes or statistical purposes</li> </ul>	<b>Article 21 UK GDPR</b>
<p>Name 5 of the countries which the European Commission has determined ensure an adequate level of protection?</p> <b>Module 8 international transfers (not in use)</b>	<p>Andorra, Argentina, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay, New Zealand and Canada (for Canada, it applies to commercial organisations only).</p>	<a href="https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/">https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/</a>
<p>What are the derogations?</p> <b>Module 8 international transfers (not in use)</b>	<p>In the absence of an adequacy decision, or of appropriate safeguards including BCRs, the GDPR contains a number of derogations that permit data controllers to transfer personal data outside the EU in specific circumstances:</p>	<b>Article 49</b>

	<p>if the data subject has consented (and been informed of the risks due to the absence of an adequacy decision and appropriate safeguards);</p> <p>for the performance of a contract;</p> <p>if the transfer is necessary for important reasons of public interest (based in law) for the exercise or defence of legal claims;</p> <p>if it's in the data subject's vital interests; or</p> <p>if the transfer is made from a register which is intended to provide information to the public and is open to consultation.</p> <p>However, public authorities will not be able to rely on the consent or contract derogations to transfer data when exercising their public powers</p>	<p><b>Article 49(3)</b></p>
<p>What are exemptions? <b>Module 9 question sheet - Exemptions</b></p>	<p>Exemptions affect or restrict the application of the GDPR. The exemptions are covered in the DPA 2018.</p> <p>The exemptions are necessary for different reasons:</p> <ul style="list-style-type: none"> <li>• The nature of the data.</li> <li>• The purpose of processing the data.</li> </ul>	<p><a href="https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/">https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/</a></p>



<p>Describe the Crime and Taxation exemption.  <b>Module 9 question sheet</b>  <b>- Exemptions</b></p>	<p>The listed GDPR provisions and Article 34 (breach reporting to the data subject) do not apply to personal data processed for any of the following purposes:</p> <ul style="list-style-type: none"> <li>a) The prevention or detection of crime;</li> <li>b) The apprehension or prosecution of offenders; or</li> <li>c) The assessment or collection of a tax or duty or an imposition of a similar nature to the extent that the application of those provisions would be likely to prejudice any of these purposes.</li> </ul> <p><b>Example</b> - An organisation (which is not a competent authority) which suspects an employee of crime may report them to the Police and does not have to explain to the DS who their personal data has been passed to (to the extent that doing so would prejudice the prevention/detection of a crime).</p> <p><b>Example</b> - If the Police asked an organisation for information about a suspect in order to detect a crime, the controller could argue that it should disclose personal data to the Police if not to do so would prejudice the prevention or detection of a crime. This is voluntary though – the organisation may refuse to disclose. (The Police might then obtain a court order in order to get the data).</p>	<p><b>Schedule 2 Part 1</b>  <b>Paragraph 2</b></p>
--	--	---

<p>Describe the legal professional privilege exemption.</p> <p><b>Module 9 question sheet - Exemptions</b></p>	<p>The listed GDPR provisions do not apply to personal data that consists of information in respect of which a claim to legal professional privilege (LPP) or, in Scotland, confidentiality of communications, could be maintained in legal proceedings. Broadly speaking, LPP applies to confidential communications between a client and their legal representative.</p> <p>Personal data in respect of which LPP (or its equivalent in Scotland) could be claimed in legal proceedings in any part of the UK does not have to be disclosed to the data subject.</p> <p>There is no prejudice test to this exemption – privileged information is always exempt from disclosure.</p> <p><b>Example</b>  An individual in a dispute with a neighbour learns that the neighbour has instructed a solicitor. The individual requests a copy of their personal data as contained in the documents sent from the neighbour to the solicitor.  The solicitor can refuse the request under LPP.</p>	<p><b>Schedule 2 Part 4 Paragraph 19</b></p>
<p>Describe the exam scripts exemption.</p> <p><b>Module 9 question sheet - Exemptions</b></p>	<p>The listed GDPR provisions do not apply to personal data consisting of information recorded by candidates during an exam. So the exemption:</p>	<p><b>Schedule 2 Part 4 Paragraph 25</b></p>

	<ol style="list-style-type: none"> <li>1. Prevents candidates from getting early access to their exam results, on the basis that the result is already going to be provided on a certain date. This stops individuals from gaining any advantage from early access, and saves exam boards from having to deal with lots of individual requests.</li> <li>2. Prevents candidates from getting copies of the answers they have given.</li> </ol> <p>However this exemption does <b>not</b> extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded. Therefore, once the results have been announced, the controller is not entitled to withhold the examination marks or marker's comments, unless other exemptions apply.</p>	
<p>Name of the <b>competent authorities</b> listed in schedule 7 of the DPA18?</p> <p><b>Module 10 quiz? DPA part 3 and 4</b></p>	<p>Any UK government department other than a non-ministerial government department, plus Scottish and Welsh Ministers, any Northern Ireland department</p> <p>Chief officers of police and other policing bodies</p>	

	<p>Other authorities with investigatory functions (eg HMRC, the Serious Fraud Office, the Financial Conduct Authority, the Health and Safety Executive)</p> <p>Authorities with functions relating to offender management (eg. probation services, the Youth Justice Board for England and Wales, a person running a prison or young offender institution)</p> <p>Other authorities (eg the director of Public Prosecutions, the ICO, a court or tribunal)</p> <p>The intelligence services (MI5, MI6 and GCHQ) are not listed as competent authorities as they are governed by the provisions in Part 4 of the DPA18.</p>	
<p>What does <b>sensitive processing</b> mean?  <b>Module 10 quiz? DPA part 3 and 4</b></p>	<p>(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;</p> <p>(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;</p> <p>(c) the processing of data concerning health;</p> <p>(d) the processing of data concerning an individual's sex life or sexual orientation</p>	<p><b>Section 35(8)</b></p>

<p>Explain the National security exemption?  <b>Module 10 quiz? DPA part 3 and 4</b></p>	<p>A wide ranging exemption which can exempt the processing from, among other things, the data protection principles and data subjects' rights (except for the requirement at principle 1 for the processing to be 'lawful' and have a lawful basis in the DPA).</p> <p>The exemption is available where required for the purposes of safeguarding national security, but the exemption must be applied as restrictively as possible consistent with the objectives of the exemption</p>	<p><b>Section 110 of the DPA 2018</b></p>
<p>In corrective measures what notices exist?  <b>Module 11 question sheet - Role and powers of the commissioner</b></p>	<p><b>Information</b> – require a controller or processor to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of carrying out the Commissioner's functions under the data protection legislation</p> <p><b>Enforcement</b> – Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—</p> <ul style="list-style-type: none"> <li>(a) to take steps specified in the notice, or</li> <li>(b) to refrain from taking steps specified in the notice,</li> </ul> <p>or both</p>	<p><b>Section 142 (1)(a) DPA</b></p> <p><b>Section 149 (1) DPA</b></p>

	<p><b>Assessment</b> – The Commissioner may by written notice (an “assessment notice”) require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation</p>	<p><b>Section 146(1) DPA</b></p>
<p>What levels of fine can we give to controllers and processors who breach data protection law?  <b>Module 11 question sheet - Role and powers of the commissioner</b></p>	<p>General conditions for imposing administrative fines; fines should be: “<b>effective, proportionate and dissuasive</b>”</p> <p>There are two levels of fine depending on the breach. They are:</p> <ul style="list-style-type: none"> <li>• £8,700,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher; or</li> <li>• £17,500,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher</li> </ul>	<p><b>Article 83 UK GDPR</b></p>
<p>What does section 132 of the DPA 2018 confer on ICO staff?  <b>Module 11 question sheet - Role and powers of the commissioner</b></p>	<p>Confidentiality of information by staff who work or have worked at the ICO. It also explains when staff at the ICO can make disclosures with legal authority</p>	

<p>What is an individual subscriber and who could this include?</p> <p><b>Module 12 question sheet – PECR and direct marketing</b></p>	<p>“individual” means a living individual and includes an unincorporated body of such individuals</p> <p>Covers individual customers, sole traders and unincorporated partnerships in England, Wales and Northern Ireland (they don’t exist in Scotland as partnerships have to be limited liability partnerships)</p>	<p><b>Regulation 2(1) PECR</b></p> <p><a href="https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/">https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/</a></p>
<p>What is a corporate subscriber?</p> <p><b>Module 12 question sheet – PECR and direct marketing</b></p>	<p>“corporate subscriber means a subscriber who is:</p> <p>(a) a company within the meaning of section 735(1) of the Companies Act 1985;</p> <p>(b) a company incorporated in pursuance of a royal charter or letters patent;</p> <p>(c) a partnership in Scotland;</p> <p>(d) a corporation sole; or</p> <p>(e) any other body corporate or entity which is a legal person distinct from its members”</p> <p>Covers subscribers that are a corporate body with separate legal status. This includes companies, limited liability partnerships, Scottish partnerships, and some government bodies</p>	<p><b>Regulation 2(1) PECR</b></p> <p><a href="https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/">https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/</a></p>
<p>What type of marketing is each of these regulations about?</p> <p>1. Reg. 19</p>	<p>1. Reg. 19 – automated calls</p> <p>2. Reg. 21 – live calls</p> <p>3. Reg. 22 – emails, SMS, voicemails</p>	

<p>2. Reg. 21 3. Reg. 22</p> <p><b>Module 12 question sheet – PECR and direct marketing</b></p>		
<p>Define direct marketing</p> <p><b>Module 12 question sheet – PECR and direct marketing</b></p>	<p>“Direct marketing” means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals</p>	<p><b>Section 122 (5) DPA 2018</b></p>
<p>How might the right to object help with marketing?</p> <p><b>Module 12 question sheet – PECR and direct marketing</b></p>	<p>As far as direct marketing is concerned, then once this right is requested it is absolute – the data subject’s personal data can’t be processed for marketing purposes. This includes the marketing itself, adding it to marketing lists or selling it for marketing by another organisation</p>	<p><b>Article 21(3) UK GDPR</b></p>



## GDPR Modules Quiz

<b>Question</b>	<b>Answer</b>	<b>Article/Recital (if applicable)</b>
Define personal data		
Define special category data		
Define a data controller		
Define a data processor		
Define a data subject		
Does UK GDPR apply to personal/domestic processing?		
Which countries could the UK GDPR apply in?		
Explain the principle of transparency		
Explain all six lawful bases for processing (one sentence each)		

Define accuracy in data protection terms		
How long should personal data be retained?		
What is data minimisation and why is it important?		
What is the accountability principle?		
When must you report a personal data breach?		
When must you inform data subjects about a personal data breach?		
What is the function of a DPIA?		
What is a subject access request?		
Why is the ability to use an access request important to a data subject?		

How do you exercise your rights?		
What is the right to be informed about? And how does it work?		
How can an individual complain?		
What is the other name for the right of erasure?		
How could personal data be rectified?		
When would you use the right to object?		
Name 5 of the countries which the European Commission has determined ensure an adequate level of protection?		
What are the derogations?		
What are exemptions?		

Describe the Crime and Taxation exemption.		
Describe the legal professional privilege exemption.		
Describe the exam scripts exemption.		
Name of the <b>competent authorities</b> listed in schedule 7 of the DPA18?		
What does <b>sensitive processing</b> mean?		
Explain the National security exemption?		
In corrective measures what notices exist?		
What levels of fine can we give to controllers and processors who breach data protection law?		

What does section 132 of the DPA 2018 confer on ICO staff?		
What is an individual subscriber?		
What is a corporate subscriber?		
What is each of these regulations about: 1. Reg. 19 2. Reg. 21 3. Reg. 22 4.		
Define direct marketing		
How might the right to object help with marketing?		

## Module 1 & 2 question sheet – introductions and definitions

Question	Answer
Define personal data	<p><b>Article 4(1) UK GDPR</b>  '<b>personal data</b>' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;</p> <p><b>Section 3(2) DPA 2018</b>  "Personal data" means any information relating to an identified or identifiable living individual</p>
Define special category data	<p><b>Article 9(1) UK GDPR</b>  Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.</p>
Define a controller	<p><b>Article 4(7) UK GDPR</b>  '<b>controller</b>' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (but see section 6 of the 2018 Act)</p>
Define a data processor	<p><b>Article 4(8) UK GDPR</b>  '<b>processor</b>' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;</p>
Define a data subject	<p><b>Article 4(1) UK GDPR</b>  See definition of personal data</p> <p><b>Section 3(5) DPA 2018</b>  "Data subject" means the identified or identifiable living individual to whom personal data relates.</p>
Does GDPR apply to personal/domestic processing?	<p><b>Article 2(2)(a) UK GDPR</b>  This Regulation does not apply to the processing of personal data:</p> <p>(a) by a natural person in the course of a purely personal or household activity;</p>
Which countries could the UK GDPR apply in?	<p><b>Article 3 UK GDPR</b></p>

	<p><b>1.</b> This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.</p> <p><b>2.</b> This Regulation applies to the processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to:</p> <p>(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom; or</p> <p>(b) the monitoring of their behaviour as far as their behaviour takes place within the United Kingdom.</p> <p><b>3.</b> This Regulation applies to the processing of personal data by a controller not established in the United Kingdom, but in a place where domestic law applies by virtue of public international law.</p>
--	---

## **GDPR Case study - module 2**

*"My wife has recently passed away. I am acting as her personal representative and have contacted her bank to obtain information about her investments. I have this morning received a letter from the bank refusing to provide me with a copy of her information. What can I do about this?"*

### **Notes**

#### Personal data definition

- Personal data is information which relates to an identified or identifiable living individual (section 3(2) Data Protection Act 2018).
- Our legislation does not apply to deceased individuals and so the Right of Access would not apply.

#### Personal representative rights

- As personal representative, this individual would likely have the right to access the information in order to deal with the wife's estate.
- This right falls outside of the legislation we regulate, so we could not assist.
- Suggest seek independent legal advice.



### **GDPR Case study - module 3**

*'I have found out that my employer has passed my personal information to HMRC without my permission. I've had a letter from HMRC and they now know where I work and how much I earn. This is personal and I didn't want anyone to know. I am really annoyed and unhappy about this as I never agreed to it. What can I do about this?'*

#### **Notes**

An organisation does not always need your consent to process or share your personal data if they can justify why they have done so. Employers have a legal obligation to disclose employee salary details to HMRC. Therefore an employer will not need your permission or consent to pass your details onto HMRC as they are relying on their legal obligation to share your data in this way.

Individuals do have a right to be informed that their personal data will be shared in this way. Therefore employers should include in privacy information what personal data will be shared with HMRC and why.

#### **Useful links**

Does an organisation need my consent?

<https://ico.org.uk/your-data-matters/does-an-organisation-need-my-consent/>

Your right to be informed if your personal data is being used

<https://ico.org.uk/your-data-matters/your-right-to-be-informed-if-your-personal-data-is-being-used/>

### Module 3 question sheet - Principles 1 – lawful processing

<b>Question</b>	<b>Answer</b>
Explain the principle of transparency	<p><b>Article 12 (1) UK GDPR</b> The controller shall take appropriate measures to provide any information referred to in <a href="#">Articles 13</a> and 14 and any communication under <a href="#">Articles 15</a> to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.</p> <p><b>Recital 39 UK GDPR</b> It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.</p> <p>The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.</p>
In one sentence for each explain all six lawful bases of processing	<p><b>Article 6 (1) UK GDPR</b> Consent Contract Compliance with a legal obligation Vital interests Public interests Legitimate interests</p>

## **GDPR Case study - module 4**

*"I was recently dismissed from my employment. The company is still holding all my personal information, for example, my bank details and sick notes. I don't believe they should still be able have these, especially after sacking me.*

*Please can help me get the company to destroy all my data immediately?"*

### **Notes**

The General Data Protection Regulation does not set any specific retention periods for personal data. However, it does state that organisations should not keep personal data for any longer than they need it.

It is likely that the organisation has a legitimate reason for retaining the personal data ("recently dismissed").

The organisation is likely to be able to justify retaining the data, for example:

- Legal obligations – financial regulations (payment details).
- May be subject to trade/industry standards of retention.
- To defend against legal claims – an individual may claim for wrongful dismissal within 6 months.

The organisation clear retention schedules and explain to individuals in privacy information how long you will retain their personal data for.

The individual has the right to erasure. This can be explained, but will not apply in the organisation has a legal obligation or legitimate reason to retain the personal data.

### **Useful links**

Right to deletion

<https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/>

## Module 4 question sheet - Principles 2 – purpose limitation

Question	Answer
<p>Define accuracy in data protection terms</p>	<p><b>Article 5(1)(d) UK GDPR</b> accurate and, where necessary, kept up to date; <b>every reasonable step must be taken</b> to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');</p> <p><b>Article 16 UK GDPR</b> The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.</p> <p><b>Section 205 DPA 2018 – definition</b> "inaccurate", in relation to personal data, means incorrect or misleading as to any matter of fact;</p>
<p>How long should personal data be retained?</p>	<p><b>Article 5(1)(e) UK GDPR</b> kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with <a href="#">Article 89(1)</a> subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');</p>
<p>What is data minimisation and why is it important?</p>	<p><b>Article 5(1)(c) UK GDPR</b> adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').</p> <p><b>Article 25(2) UK GDPR</b> The controller shall implement appropriate technical and</p>

	<p>organisational measures for ensuring that, <b>by default</b>, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p>
--	---

## **GDPR Case Study – module 5**

*"Yesterday when I went into the chemist to pick up my prescription, I noticed that they kept the prescription orders in a basket on the counter. Surely this is a breach of GDPR. I could clearly see the patient's name on the order on top of the pile as well as details of their medication. Someone could easily take the basket as the counter was left unattended and there were easily 10-20 prescriptions in there."*

### **Notes**

#### Security

- Organisations have an obligation to take appropriate measures to keep personal data secure.
- The GDPR does not set out what security measures should be taken.
- What is appropriate will depend on the type of organisation and data held – sensitive data should be given more protection.

#### Next steps

- Concerns about how the chemist has handled your personal data, should be raised with them directly.

### **Useful links**

Security (for information – don't link this guidance to individuals)

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>

Right to raise a concern:

<https://ico.org.uk/your-data-matters/raising-concerns/>

## Module 5 question sheet - Principles 3 – security

Question	Answer
<p>What is the accountability principle?</p>	<p><b>Article 5(2) UK GDPR</b> The controller shall be responsible for, and be <b>able to demonstrate</b> compliance</p> <p><b>Article 24(1) UK GDPR</b> Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able <b>to demonstrate that processing is performed in accordance with this Regulation</b>. Those measures shall be reviewed and updated where necessary.</p>
<p>When must you report a personal data breach?</p>	<p><b>Article 33(1) UK GDPR</b> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.</p>
<p>When must you inform data subjects about a personal data breach?</p>	<p><b>Article 34(1) UK GDPR</b> When the personal data breach <b>is likely to result in a high risk</b> to the rights and freedoms of natural persons, the controller shall <b>communicate</b> the personal data breach to the data subject without undue delay.</p>
<p>What is the function of a DPIA?</p>	<p><b>Article 35(1) UK GDPR</b> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is <b>likely to result in a high risk</b> to the rights and freedoms of natural persons, the controller</p>

	shall, prior to the processing, carry out an <b>assessment of the impact</b> of the envisaged processing operations on the protection of personal data.
--	---



## **GDPR Case study - module 6**

*"A local food bank has sent me a letter about how I can apply for weekly food parcels if I need them. I have never spoken to them before. They clearly have information about me but I don't know where they got it from or what they know about me. What can I do about it?"*

### **Notes**

Individuals have a right to make a subject access request (SAR). Under a SAR individuals:

- Can ask for a copy of all personal data held about them.
- Can ask an organisation where their personal data was obtained from.

### **SARs**

- Can be made verbally (we advise to make it in writing)
- Free of charge.
- DC's can ask for proof of identity.
- DC's can ask for more information to comply with request.
- DCs should respond within one month.

### **Useful links**

Right to get copies of your data:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>

## Module 6 question sheet - Individual rights – part 1

Question	Answer
What is an access request?	<p><b>Article 15(1) UK GDPR</b> The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, <b>access</b> to the personal data</p>
Why is the ability to use an access request important to a data subject?	<p><b>Recital 63 UK GDPR</b> A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.</p>
How do you exercise your rights?	<p><b>Article 12(2) UK GDPR</b> The controller shall facilitate the exercise of data subject rights under <a href="#">Articles 15</a> to 22. In the cases referred to in <a href="#">Article 11(2)</a>, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under <a href="#">Articles 15</a> to 22, unless the controller demonstrates that it is not in a position to identify the data subject.</p> <p><b>Note:</b> GDPR is silent on how an individual exercises their rights – this means any method is appropriate including verbal requests.</p>
What is the right to be informed about? And how does it work?	<p><b>Article 5(1)(a) UK GDPR</b> Personal data shall be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');</p> <p><b>Article 13 UK GDPR</b> Information to be provided where personal data are collected from the data subject – <b>to be given at the time of collection</b></p> <p><b>Article 14 UK GDPR</b> Information to be provided where personal data have not been obtained from the data subject – <b>to be given</b></p>

	<p>within a reasonable period after obtaining the personal data, but at the latest within one month</p>
How can an individual complain?	<p><b>Article 77(1) UK GDPR</b> Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Commissioner if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.</p>

## **GDPR Case Study – Module 7**

*'Following a dispute with a neighbour, we were visited by a housing officer from the Housing Association we rent our property from. They interviewed us with regard to our complaint. We applied for a 'subject access review' and following the receipt of the officer's notes on the interview we made an official complaint.*

*The record contains a number of inaccurate and misleading statements.*

*Following an investigation the matter was passed to the data protection team and we received what in our opinion is a very poor response that is not in line with GDPR 2018.*

*Our complaint is as follows:*

- 1. The Housing Association have refused as far as can be ascertained from the letter to delete this incorrect information.*
- 2. We believe that it is a refusal to deletion and as such should have a detailed and clear list of reasons for the refusal in line with the current Regulations.*

*As you will appreciate we have a number of documents connected to this matter and subject to your request can make any document available via the electronic system, provided you are happy that electronic copies are acceptable.'*

### **Notes**

The GDPR gives individuals the right to request erasure.

- Right to erasure is not absolute if the Housing Association can justify why they need to retain the record.
- The Housing Association should explain why the record cannot be deleted if it can't.

The GDPR places the obligation on the data controllers to ensure personal data is accurate.

- Individuals do have the right to request inaccurate data is corrected.
- Records may be an opinion rather than fact.
- Housing Association may offer the opportunity to add supplementary notes against the disputed record.

Individual should go back to the Housing Association and try and resolve their concern.

## **Useful links**

Right to erasure :

<https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/>

Right to have inaccurate data corrected:

<https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected/>

Raising a concern with an organisation:

<https://ico.org.uk/your-data-matters/raising-concerns/>

## Module 7 question sheet - Individual rights – part 2

<b>Question</b>	<b>Answer</b>
What is the other name for the right of erasure?	<b>Article 17 UK GDPR</b> Right to be forgotten
How could personal data be rectified?	<b>Article 16 UK GDPR</b> The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
When would you use the right to object?	<b>Article 21 UK GDPR</b>  <b>Absolute right:</b> <ul style="list-style-type: none"><li>• direct marketing purposes</li></ul> <b>Qualified right:</b> <ul style="list-style-type: none"><li>• the use of information society services</li><li>• for scientific or historical research purposes or statistical purposes</li></ul>

## **GDPR Case study - module 8**

*"The company that I work for has recently outsourced the payroll duties to another company in France. It really worries me that my personal data and payment details are being used by a company in another country. I obviously have no idea how the law works in France, but I am guessing they can do whatever they want with it, without me even knowing."*

### **Notes**

Transfers of personal data to countries in the European Economic Area are subject to the General Data Protection Regulations.

France is in the European Economic Area.

The personal data must therefore be processed in accordance with all of the GDPR principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).

Do "payroll duties" involve the processing of personal data? The French company may not actually be processing any personal data.

The individual should be directed to raise any concerns, and seek clarity/reassurance from their employer.

## **GDPR Case study - module 9**

*"I have recently been a little bit of trouble with the Police. I have reason to believe that they got my address and contact details from my employer. I am disgusted that; a) the Police can do this, b) my employer have just given them my details, and c) nobody has told me this has happened. What can I do about this?"*

### **Notes**

There is an exemption that allows organisations to disclose personal data for the purpose of crime and taxation.

- Schedule 2. Part 1. Paragraph 2.
- The exemption is permissive – organisations are not obliged to disclose the information.
- A court order would compel the organisation to disclose the information.

The Crime and Taxation provision exempts the organisation from the requirements to inform the data subject, to the extent that informing them would prejudice the purpose for which it is being processed.

The organisation needs to be satisfied that the request is legitimate.

- Request should be in writing.
- Organisation should keep a record of what is being disclosed and justification for doing so.



## **GDPR Case Study – Module 10**

I was also recently involved in a fight outside a club. The police are making enquiries and I have been told that they have got the CCTV footage from outside the club. I am not happy that they have got those images of me and I was not told about this – can they do that? I thought GDPR says you have to be told when someone has your information?

I feel like they are going to lay the blame on me for the fight. Am I able to request a copy of the statements and CCTV footage they have in relation to the incident?

### **Notes**

GDPR does not apply to data processed for law enforcement purposes by competent authority – this processing falls within Part 3 of DPA 2018.

Right to be informed

Individual can raise this as a concern with police however should be made aware of the following;

- Restrictions to this right if informing individual would prejudice investigations.
- Must be and justified by police if restriction applied.

Right of access

Individual can make request for CCTV footage but should be made aware of the following;

- Right of access can be restricted if to comply would prejudice investigation of crime.
- Must be justified by police if restriction applied.

### **Useful links**

Your data Matters – ‘Your data held by the police’ -

<https://ico.org.uk/your-data-matters/crime/>

## **GDPR Case Study – Module 11**

I've been the victim of a data breach by a large international organisation. They have leaked my data along with thousands of others which has been widely publicised in the media. I have complained to the organisation who have given me their final response and directed me to your office if I am not happy, which I am not. How do I bring this complaint to you?

What are you actually going to do about my complaint? What legal powers do you have to make sure this organisation is complying with the data protection law?

Can you fine them and if so how much? They need to pay for what they have done. I want compensation too.

### **Notes**

#### Complaint

- Individual has the right to make complaint to us for assessment. Should be directed to make a complaint section of website.

#### Legal powers to enforce

- Commissioner has legal powers to issue Enforcement Notice and issue monetary penalties where appropriate. Expectations should be managed by stating that each complaint is assessed on a case by case basis and legal action is only taken in most serious cases.

#### Fines

- There are different levels of fines based on size and turnover of organisation. Level of fine decided on a number of factors and should be proportionate to the infringement.
- No power to award or involvement in claims for compensation – should take legal advice.
- 

### **Useful links**

How to make a complaint - <https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>

How we handle complaints - <https://ico.org.uk/about-the-ico/what-we-do/how-we-handle-concerns/>

## **GDPR Case Study Module 12**

### **Notes**

#### **Live marketing calls**

- Regulation 21 of the PECR provides that live marketing call should not be made to individuals who have registered with the TPS (or CTPS)
- unless the person has specifically consented to the calls – even if they are existing customers. Or to anyone who has told you that they don't want to receive marketing calls.

#### Claims management calls

- An organisation must have your consent if it wants to make live marketing calls to you about claims management services (for example about claiming back PPI, personal injury claims, claims about sickness whilst you were on holiday etc).

#### Right to object

- Individuals exercise their right to object to marketing (right to prevent processing for the purpose of marketing).
- Only relevant where the individual has identified the organisation and the organisation has called them using their name.

#### Response

- In a lot of these cases it will be necessary to 'empathise' with individuals.
- Cannot stop or block unwanted nuisance calls – suggest that individuals may wish to contact their service provider who may be able to provide a facility to enable them to block the calls coming through to them.
- Unable to look in to individual concerns about nuisance marketing calls
- Online Reporting Tool which enables individuals to report organisations directly to us and that this information is used by us to identify and locate organisations responsible for making unsolicited marketing calls.
- If relevant, encourage individuals to register with the TPS.
- Individuals should not respond to any instruction given in an automated message such as pressing any particular key on their telephone key pad.

#### **Useful links:**

Guidance on telephone marketing:

<https://ico.org.uk/your-data-matters/nuisance-calls/>

Reporting Tool:

<https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/>

TPS website:

<https://complaints.tpsonline.org.uk/consumer>

Art 21 – preventing direct marketing

<https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/>

## Case Study 1

Ms V, manager of Big Cheese Ltd, receives a visit from the Police asking for the IP address of the computer used by one of her employees, and the logging in/out times, for the previous day.

The Police advise Ms V that they are investigating an alleged computer hack which they suspect was committed by the employee in question from one of Big Cheese's computers yesterday.

The Police also ask for the employee's entire HR record in case it is useful. What information should the Police be able to see? What does Ms V need to consider?

What difference does it make if the Police have a Court Order for the information?

## Answer

Ms V can consider whether to disclose the information.

**Schedule 2 Part 1 Paragraph 2(1)** is relevant. The listed GDPR provisions do not apply to personal data processed for any of the following purposes –  
(a) the prevention or detection of crime,  
(b) the apprehension or prosecution of offenders, or  
(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,  
to the extent to which the application of those provisions to the data would be likely to prejudice any of these purposes.

The listed GDPR provisions in this Part include the fairness and transparency elements of Article 5(1)(a) (lawful, fair and transparent processing) and Article 5(1)(b) (purpose limitation).

Ms V must first consider the extent to which compliance with her obligations under principle (a) (fairness, transparency, fair processing information) and principle (b) (using the data for a different purpose) would be likely to prejudice the prevention and detection of crime. After this consideration, she may choose to apply the exemption if its application is justified. Therefore if it would be likely to prejudice the detection of a crime to refuse to provide this information, Ms V may disclose the personal data to the Police.

However Ms V still needs a lawful basis for processing the data (a disclosure is a type of processing). She will be able to rely on the Article 6 basis legitimate interest but will also need an Article 10 legal or official authority for processing. Her legal authority is likely to be **Schedule 1 Part 2 Condition 10(1) of the DPA2018:**

### **Preventing or detecting unlawful acts**

This condition is met if the processing—

- a) is necessary for the purposes of the prevention or detection of an unlawful act,
- b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and
- c) is necessary for reasons of substantial public interest.

She should ask the Police to confirm the information that is necessary for the investigation. The information relating to IP addresses and login times is clearly relevant to the investigation, and there is no other way for the police to get this information. However, it is less likely that the HR file is relevant, and it contains a lot of sensitive information such as a medical record. Ms V can probably disclose the IP address and login times, but not the full HR file.

Ms V should get a request in writing from the Police, and keep a note of what she discloses.

She should ask the Police whether it is necessary to withhold the facts of the disclosure from the employee. If telling him would prejudice the investigation, then under this exemption, she is under no obligation to do so.

If the Police have a Court Order for the information, the exemption at **Schedule 2, Part 1, Paragraph 5(2)** may apply if complying with the listed provisions would prevent the disclosure.

## Case Study 2

You are an HR officer for a company that has been asked to provide a reference for a former employee. The reference is written but before it is sent, the employee emails you asking to be provided with a copy of the contents so they can check it is accurate. What rights under the GDPR does the individual have to see the information?

### Answer

The reference contains information relating to the former employee, including expressions of opinion about them and will be likely to be their personal data under the GDPR.

The company may decide to just give out the reference.

However under **Schedule 2 Part 4 Paragraph 24**, the listed GDPR provisions do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of:

- a) the education, training or employment (or prospective education, training or employment) of the data subject,
- b) the placement (or prospective placement) of the data subject as a volunteer,
- c) the appointment (or prospective appointment) of the data subject to any office, or
- d) the provision (or prospective provision) by the data subject of any service.

The listed GDPR provisions in this Part include Article 15 which covers the right of access by the data subject.

Therefore the organisation which gives a reference is exempt from the obligation to provide a copy of their personal data to the data subject.

The recipient organisation may also use the exemption.

### Case study 3

Miss G has taken her 'A' levels but is not happy with the grade awarded for her History exam. She has therefore submitted an access request and asked the relevant examination board to provide her with both her examination scripts and any moderation remarks recorded about her paper. What does the examination board have to provide?

What difference does it make if the access request is made before the examination results are announced?

### Answer

Information comprising the answers given by a candidate during an examination is exempt from the right of subject access under **Schedule 2 Part 4 Paragraph 25(1)**. This states that:

(1) The listed GDPR provisions do not apply to personal data consisting of information recorded by candidates during an exam.

Therefore an access request made under Article 15 cannot be used to obtain a copy of an individual's examination script.

However this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded.

Once the results have been announced, the controller is not entitled under the GDPR to withhold the marker's comments on the exam papers or comments concerning any moderation which has taken place (unless other exemptions under the GDPR apply).

This applies by virtue of **Schedule 2 Part 4 Paragraph 25(2)** which states that personal data which consists of **marks or other information processed by a controller**

- a) for the purposes of determining the results of an exam, or
- b) in consequence of the determination of the results of an exam,

should be provided to the data subject within certain time limits, depending on the date of the request and the announcement of the results.

If the request is made before the examination results are available, the timescales for the response to the request are modified – either 5 months or, if earlier, 40 days after the results are announced.



## **Knowledge Builder Quiz (Answers)**

The following questions and answers are all based around the information available on [Knowledge Builder](#).

### **1. What would a controller need to do to decide if legal professional privilege applies?**

*To decide whether legal professional privilege applies, a controller receiving a SAR would need to:*

- *look at each document containing the personal data of the DS;*
- *identify who the parties to the 'confidential communication' are; and*
- *that legal action is possible or probable (where litigation privilege is being claimed).*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs-and-LPP.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs-and-LPP.aspx)

### **2. Which legislation requires Companies House to make the names and addresses of company directors public? Do company directors have to provide their residential address?**

*The Companies Act 2006 places a statutory obligation on Companies House to make names and addresses of company directors public. Directors can provide a 'service address' to appear on the public record, with their residential address restricted only to specified regulatory bodies and credit reference agencies.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Personal%20data/Companies-house,-disclosure-of-directors.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Personal%20data/Companies-house,-disclosure-of-directors.aspx)

### **3. Will a private individual be a controller for a self-employed person contracted to perform certain tasks for them, for example a plumber replacing a faulty water heater?**

*No, in these circumstances the private individual will not be a controller. This is because the plumber is contracted in the course of a purely personal/household activity.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/Individuals-as-controllers.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/Individuals-as-controllers.aspx)

#### **4. Can a third party make a subject access request on someone else's behalf using a power of attorney?**

*Yes, in certain circumstances.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/Power-of-Attorney-and-SARs.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/Power-of-Attorney-and-SARs.aspx)

#### **5. Which piece of legislation allows the DVLA to disclose a vehicle's driver information? What must those third parties who wish to receive the information show?**

*Road Vehicles Regulations Act 2002.*

*The third parties must show they have a reasonable cause to receive it. What is a reasonable cause would have to be considered on a case by case basis.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/DP%20basics%20and%20definitions/DVLA-disclosing-driver-details.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/DP%20basics%20and%20definitions/DVLA-disclosing-driver-details.aspx)

#### **6. Where does the money go from fines for non-payment of the data protection fee by organisations?**

*The ICO doesn't keep any of the money received from fines; this goes to the Treasury and into the public purse.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Our%20role/Non-payment-of-data-protection-fee.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Our%20role/Non-payment-of-data-protection-fee.aspx)

#### **7. The UK GDPR says that the time limit for responding to a SAR can be extended if the SAR is complex. What makes a SAR complex?**

*The UK GDPR doesn't define this. It will be dependent on the circumstances in each case. The size and resources of an organisation will be determining factors, as will:*

- *Any technical challenges in retrieving the information,*
- *Where there are any exemptions,*
- *Clarifying any potential issues about whether information should be disclosed about a child to someone with parental responsibility, and*

- *Any specialist work needed to provide the information in an eligible form.*
- *Volume may add to the complexity but is not enough on its own.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/Complex-SARs.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/Complex-SARs.aspx)

### **8. If an organisation is using my work email address and it contains my name, will it be personal data?**

*Yes, if it can be used to identify you. It does not need to include a full name, an initial or surname may be enough.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Personal%20data/Emails-and-personal-data.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Personal%20data/Emails-and-personal-data.aspx)

### **9. A company posted me my SAR using Royal Mail and it was delivered to a neighbour's address instead of mine, even though the address was correct on the envelope. Is this a data breach by the postman?**

*No, a postman or courier misreading the address on the envelope and delivering it to the wrong address isn't processing personal data and so would not be considered a personal data breach under the UK GDPR. The customer may be able to raise a service complaint with the Royal Mail but not a DP complaint.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/Postal%20delivery%20and%20controllership.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/Postal%20delivery%20and%20controllership.aspx)

### **10. A 'Youtuber' has posted a video which has been viewed by thousands of people and which names a number of individuals. Will the person who made and posted the video be subject to data protection legislation?**

*It is unlikely that posting a video with the intention of making it available to 'an indefinite number of people' would fall under purely personal or household activities and so the Youtuber would be within the scope of UK GDPR.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/YouTube-as-a-controller.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/YouTube-as-a-controller.aspx)

## **11. Can the Danish Standard Contract Clauses (SCCs) be used to satisfy international transfer obligations?**

*The Danish SCCs are a standard processor agreement, which help organisations meet their requirements when using a processor (article 28). They relate to the content of the contract between controller and processor and mean that any such contract will be compliant.*

*However, they are very different to the European Commission SCCs which relate to international transfers. An organisation will therefore need to ensure they adopt the European Commission SCCs in addition to the Danish SCCs if the relationship between controller and processor involves international transfers.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/International%20transfers/Danish-SCCs-and-international-transfers.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/International%20transfers/Danish-SCCs-and-international-transfers.aspx)

## **12. Does a school need to provide an teacher assessments when requested? Has this been affected by the Pandemic?**

*A student can exercise their right of access to request their personal data contained within teacher assessment of examiner comments. However, a school is not obliged to provide this until the exam results are published. This is in line with exemption under DPA18 (Schedule 2, Part 4, Paragraph 25(2)).*

*The timeframe for responding to these request are either:*

- Within 5 months of receiving the request; or*
- Within 40 days of announcing the exam results, whichever data is earliest.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs-and-exam-scripts.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs-and-exam-scripts.aspx)

*This exemption still applies regardless of any changes in the exam process due to the pandemic.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Coronavirus/Exam-scripts-and-COVID-19.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Coronavirus/Exam-scripts-and-COVID-19.aspx)

### **13. How should an organisation provide privacy information when recording telephone calls?**

*Controllers don't have to give individuals all the necessary privacy information directly to individuals during the call. However, they must tell people the most important information – namely that the call is being recorded and the reason for this.*

*The controller could provide the rest of the information (the retention period for the personal data, individual rights available, who it will be shared with etc) by different means, such as sending a copy of the privacy notice by email or actively providing a link to their online privacy policy. Simply putting privacy information on a website without letting anyone know where it is won't meet GDPR requirements.*

*This layered approach is one of a number of different techniques controllers can use.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20to%20be%20informed/Privacy-information-and-call-recordings.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20to%20be%20informed/Privacy-information-and-call-recordings.aspx)

### **14. What are the timescales for dealing with requests for educational information from parents? Does this apply to all schools?**

*There are two distinct rights to information held about pupils by schools - the pupil's right of access under the GDPR and the parent's own separate right of access to their child's 'educational record'.*

- *Schools have to respond to requests for a child's educational record within 15 school days.*
- *Schools have to respond to requests for all other personal data held about a child within a calendar month.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs,-parents-and-education-information.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs,-parents-and-education-information.aspx)

*It is important to note that Parents can't generally access their child's educational record from a non-maintained school. Also, different regulations across the UK provide for parents' access to certain information as follows:*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/Parents-accessing-education-information.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/Parents-accessing-education-information.aspx)

**15. I have just received an erasure request from an individual. What do I need to tell the individual?**

*Organisations should have a policy setting out how they will deal with erasure requests. This should explain what's involved in the process.*

*For example, they may be able to delete information from live systems straight away. It could take a little longer for information to be removed from back-up systems or overwritten.*

*Until then organisations must have appropriate security measures in place to protect the personal data and make sure its not used for anything else.*

*There are circumstances when an organisation might refuse to erase personal data. They should explain why to the individual and let them know about their rights to complain to the ICO.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Personal%20data/Proof-of-erasure-of-personal-data.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Personal%20data/Proof-of-erasure-of-personal-data.aspx)

**16. I am a DPO, and have received a request from an individual. Do I need to deal with this personally?**

*No, they don't. It's part of the DPO's role to assist the organisation with ensuring information rights compliance and this can include providing staff with advice on handling requests from individuals, such as SARs.*

*This doesn't prevent a DPO from handling more routine requests (eg this could form part of the tasks assigned to them under another role they hold within the organisation) – so long as this doesn't present a conflict of interest or mean their main data protection duties as a DPO take a secondary role to business interests.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/DP%20basics%20and%20definitions/DPOs-and-handling-requests-from-individuals-.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/DP%20basics%20and%20definitions/DPOs-and-handling-requests-from-individuals-.aspx)

**17. My company has recently gone in to liquidation. Do I still need to deal with subject access requests?**

*The duty to comply with data protection provisions, including the rights of individuals to subject access and the ability to take advantage of the exemptions, continue to apply to the company throughout the liquidation. These obligations only cease once the company has been fully dissolved.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs-and-liquidation.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Right%20of%20access/SARs-and-liquidation.aspx)

**18. I own a small shop and have recently received a subject access request for CCTV footage from an individual. The footage includes other people. What do I do?**

*Although organisations may sometimes be able to disclose information relating to a third party who is included in CCTV footage, they need to decide whether it's appropriate to do so on a case by case basis.*

*As our guidance explains, this involves balancing the data subject's right of access against the other individual's rights relating to their own personal data.*

*There's no hard and fast rule about when third party information should be redacted, and it's not our role to explain exactly to organisations how this should be done. It's an important factor that organisations should consider when they are selecting a CCTV package to use. We don't consider that reasons like the length of time it takes to redact the footage, or how complexity a process it is, are appropriate reasons for organisations not to do it when they should.*

[https://indigooffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/CCTV%20and%20redaction.aspx](https://indigooffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Controllers%20and%20processors/CCTV%20and%20redaction.aspx)

**19. Do I need to share/report coronavirus results of my staff with test and trace?**

*Yes, there's now a legal obligation for the results of tests to be reported into NHS Test and Trace.*

*It's not just those that show positive results, but also those which come back as negative or void.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Coronavirus/Organisations-reporting-test.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Coronavirus/Organisations-reporting-test.aspx)

## **20. Do I need to do anything different with children's data?**

*Any organisation collecting and processing children's personal data must think about the need for extra protection and design their systems and processes with this in mind.*

*Privacy notices must be clear. Children should find it easy to understand what will happen with their personal data, and what rights they have. Children have the same rights as adults over their personal data.*

*If the controller wants to rely on consent as a lawful basis for processing, when offering an online service directly to a child, in the UK only children aged 13 or over are able to provide their own consent.*

*For children under this age the controller has to get consent from whoever holds parental responsibility for the child - unless the online service offered is a preventive or counselling service.*

*The Age Appropriate Design Code is a data protection code of practice for providers of online services likely to be accessed by children. It contains standards that we expect providers to meet when they process children's personal data.*

[https://indigoffice.sharepoint.com/sites/TGrp\\_KnowledgeCentre\\_CorporateAffairsandGovernance/SitePages/Personal%20data/Children-and-personal-data.aspx](https://indigoffice.sharepoint.com/sites/TGrp_KnowledgeCentre_CorporateAffairsandGovernance/SitePages/Personal%20data/Children-and-personal-data.aspx)



## Law Enforcement Processing quiz

The aim of this quiz is to help staff understand Part 3 of the Data Protection Act 2018. All the answers to these questions can be found on our website, specifically, [in the Guide to Law Enforcement Processing](#). Staff can point customers to these areas when they are in contact with them.

Question	Answer	Website section
<b>Law Enforcement Processing</b>		
Who does Part 3 Apply to?	Part 3 only applies to competent authorities (or their processors) processing for criminal law enforcement purposes.	For organisations > Guide to LE Processing > Scope and key definitions  <a href="https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/">https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/</a>
Who are competent authorities?	A competent authority means: <ul style="list-style-type: none"> <li>• a person specified in Schedule 7 of the DPA 2018; or</li> <li>• any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.</li> </ul>	For organisations > Guide to LE Processing > Scope and key definitions <a href="#">Scope and key definitions   ICO</a>
Does Part 3 apply to all of the data processing a competent authority does?	No, any processing carried out by a competent authority which is not for the primary purpose of law enforcement will be covered by the general processing regime under part 2 of the DPA 2018 (read with the UK GDPR).	For organisations > Guide to LE Processing > Scope and key definitions <a href="#">Scope and key definitions   ICO</a>
How does the first principle of Part 3 differ from the first principle of GDPR?	Transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation in certain circumstances.	For organisations > Guide to LE Processing > Principles  <a href="#">Principles   ICO</a>
What does the fourth principle require organisations to categorise?	They must be able to distinguish data between different categories of individuals, such as suspects; individuals who have been convicted; victims and witnesses.	For organisations > Guide to LE Processing > Principles  <a href="#">Principles   ICO</a>

<p>What does 'strictly necessary' mean, in the context of sensitive processing?</p>	<p>Strictly necessary in this context means that the processing has to relate to a pressing social need, and they cannot reasonably achieve it through less intrusive means.</p>	<p>For organisations &gt; Guide to LE Processing &gt; Conditions for sensitive processing  <a href="#">Conditions for sensitive processing   ICO</a></p>
<p>To process sensitive data under Part 3, what conditions may you need to satisfy?</p>	<p>One of the conditions in Schedule 8</p> <ul style="list-style-type: none"> <li>• necessary for judicial and statutory purposes – for reasons of substantial public interest;</li> <li>• necessary for the administration of justice;</li> <li>• necessary to protect the vital interests of the data subject or another individual;</li> <li>• necessary for the safeguarding of children and of individuals at risk;</li> <li>• personal data already in the public domain (manifestly made public);</li> <li>• necessary for legal claims;</li> <li>• necessary for when a court acts in its judicial capacity;</li> <li>• necessary for the purpose of preventing fraud; and</li> <li>• necessary for archiving, research or statistical purposes.</li> </ul>	<p>For organisations &gt; Guide to LE Processing &gt; Conditions for sensitive processing  <a href="#">Conditions for sensitive processing   ICO</a></p>
<p>Is there any other way to process sensitive data?</p>	<p>Yes, it can also be processed based on consent</p>	<p>For organisations &gt; Guide to LE Processing &gt; Conditions for sensitive processing  <a href="#">Conditions for sensitive processing   ICO</a></p>
<p>What is an appropriate policy document?</p>	<p>An appropriate policy document must explain:</p> <p>(a) your procedures for ensuring compliance with the law enforcement data protection principles; and</p> <p>(b) your policies on the retention and erasure of this data.</p>	<p>For organisations &gt; Guide to LE Processing &gt; Conditions for sensitive processing  <a href="#">Conditions for sensitive processing   ICO</a></p>
<p>Which individual rights do not exist under Part 3?</p>	<p>The right to object and the right to data portability, do not exist in Part 3 of the Act.</p>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights  <a href="#">Individual rights   ICO</a></p>

<p>What type of information do the rights not apply to?</p>	<p>'Relevant personal data' , which is personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.</p>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights <a href="#">Individual rights   ICO</a></p>
<p>What information must be provided to individuals about the processing of their data?</p>	<p>You must make this information generally available to the public:</p> <ul style="list-style-type: none"> <li>• your identity and contact details;</li> <li>• the contact details of your data protection officer, if applicable;</li> <li>• purposes of the processing;</li> <li>• the individual's rights (access, rectification, erasure and restriction); and</li> <li>• the right to lodge a complaint with the Information Commissioner and the contact details of the ICO.</li> </ul>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; The right to be informed <a href="#">The right to be informed   ICO</a></p>
<p>Is there a right to further processing information?</p>	<p>Yes, there is also a right to:</p> <ul style="list-style-type: none"> <li>• your legal basis for processing;</li> <li>• your retention period or the criteria you used to determine the retention period;</li> <li>• any recipient or categories of recipients of the personal data (including in third countries or international organisations); and</li> <li>• any further information needed to enable individuals to exercise their rights, eg if information is collected without their knowledge subject to restrictions that prevent any prejudice to an ongoing investigation or compromise to operational techniques</li> </ul>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; The right to be informed <a href="#">The right to be informed   ICO</a></p>
<p>When can organisations limit the information in their responses to individual rights requests?</p>	<p>They may restrict the provision of further information where it is necessary and proportionate to:</p> <ul style="list-style-type: none"> <li>• avoid obstructing an official or legal inquiry, investigation or procedure;</li> <li>• avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;</li> </ul>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; The right to be informed <a href="#">The right to be informed   ICO</a></p>

	<ul style="list-style-type: none"> <li>• protect public security;</li> <li>• protect national security; or</li> <li>• protect the rights and freedoms of others.</li> </ul>	
Can an organisation extend the time for responding to a subject access request/other individual rights requests?	<p>They must provide the information requested without delay and at the latest within one calendar month, from the first day after the request was received.</p> <p>Unlike the GDPR, they are not able to extend the period of compliance by a further two months if requests are complex or numerous.</p>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; The right of access</p> <p><a href="#">The right of access   ICO</a></p>
When must an organisation restrict the processing of personal data?	<p>They are required to restrict the processing of personal data for the law enforcement purposes in two situations:</p> <ul style="list-style-type: none"> <li>• If they must maintain personal data for the purposes of evidence.</li> <li>• If an individual contests the accuracy of personal data but it is not possible to be certain about its accuracy.</li> </ul>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; The right to erasure and restriction</p> <p><a href="#">The right to erasure and the right to restriction   ICO</a></p>
When can an organisation take a significant decision by solely automated means?	<p>Only when that decision is required or authorised by law</p>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; The right not to be subject to automated decision-making</p> <p><a href="#">Right not to be subject to automated decision-making   ICO</a></p>
Can individual rights requests be refused?	<p>Yes, they may refuse to respond to a request if it is manifestly unfounded or excessive, or charge a reasonable fee for dealing with it.</p>	<p>For organisations &gt; Guide to LE Processing &gt; Individual rights &gt; Manifestly unfounded and excessive requests</p> <p><a href="#">Manifestly unfounded and excessive requests   ICO</a></p>

<p>What obligations do organisations have to document their processing activities?</p>	<p>They must maintain internal records of processing activities including:</p> <ul style="list-style-type: none"> <li>• your name and details (and where applicable those of other controllers, your representative and data protection officer);</li> <li>• purposes of your processing;</li> <li>• description of the categories of individuals and categories of personal data;</li> <li>• categories of recipients of personal data;</li> <li>• details of transfers to third countries including documentation of the transfer mechanism safeguards in place;</li> <li>• your retention schedules; and</li> <li>• a description of your technical and organisational security measures.</li> </ul>	<p>For organisations &gt; Guide to LE Processing &gt; Accountability and governance &gt; Documentation</p> <p><a href="#">Documentation   ICO</a></p>
<p>What logs must an organisation keep for their IT databases?</p>	<p>If they operate automated processing systems (any IT database), they must keep logs for at least the following processing actions:</p> <p>Collection</p> <p>Alteration</p> <p>Consultation</p> <p>Disclosure (including transfers)</p> <p>Combination</p> <p>Erasure</p>	<p>For organisations &gt; Guide to LE Processing &gt; Accountability and governance &gt; Logging</p> <p><a href="#">Logging   ICO</a></p>
<p>What is the purpose of logging?</p>	<p>To enable them to monitor and audit internal processing, and also enables them to monitor systems for inappropriate access and/or disclosure of data, to</p>	<p>For organisations &gt; Guide to LE Processing &gt; Accountability and governance &gt; Logging</p> <p><a href="#">Logging   ICO</a></p>

	verify the lawfulness of any processing, and to ensure the integrity and security of personal data.	
Do all organisations need a data protection officer?	Under Part 3 they must appoint a data protection officer (DPO) unless they are a court, or other judicial authority acting in a judicial capacity.	For organisations > Guide to LE Processing > Accountability and governance > Data protection officers  <a href="#">Data protection officers   ICO</a>
What personal data breaches need to be reported to the ICO under Part 3?	They only have to notify the relevant supervisory authority of a breach if it is likely to result in a risk to the rights and freedoms of individuals.	For organisations > Guide to LE Processing > Personal data breaches  <a href="#">Personal data breaches   ICO</a>
What are the three conditions for an international transfer?	<p>The transfer has to be necessary for any of the law enforcement purposes.</p> <p>The transfer has to be based on either a finding of adequacy in respect of the third country, or where other appropriate safeguards are in place, or if not, that the transfer is for certain specified special circumstances.</p> <p>The transfer is to a relevant authority in the third country, or is a 'relevant international organisation' ie an international body that carries out functions for any of the law enforcement purposes.</p>	For organisations > Guide to LE Processing > International transfers  <a href="#">International transfers   ICO</a>
What are the five special circumstances that organisations can transfer data under if there is no adequacy and no appropriate safeguard?	<ol style="list-style-type: none"> <li>1. To protect the vital interests of the data subject or another person;</li> <li>2. To safeguard the legitimate interests of the data subject;</li> <li>3. For the prevention of an immediate and serious threat to the public security of a member state or third country;</li> <li>4. In individual cases for any of the law enforcement purposes; or</li> </ol>	For organisations > Guide to LE Processing > International transfers  <a href="#">International transfers   ICO</a>

	5. In individual cases for a legal purpose.	
What are the four conditions to meet if the transfer isn't to a relevant authority?	<ol style="list-style-type: none"> <li>1. The transfer is strictly necessary in a specific case, for the performance of a task by the transferring controller, as provided by law for any of the law enforcement purposes.</li> <li>2. The fundamental rights and freedoms of the data subject do not override the public interest concerning the transfer.</li> <li>3. The transferring controller considers that the transfer to a relevant authority in the third country would be ineffective, or inappropriate.</li> <li>4. The transferring controller sets out the specific purposes for which the data may be processed by the intended recipient and informs them of these.</li> </ol>	<p>For organisations &gt; Guide to LE Processing &gt; International transfers  <a href="#">International transfers   ICO</a></p>

## DEFINITIONS

<b>What does PECR cover?</b>	<ul style="list-style-type: none"> <li>• Electronic marketing;</li> <li>• Cookies or similar;</li> <li>• Security of public electronic communications services;</li> <li>• Privacy of customers using communications networks or services:               <ul style="list-style-type: none"> <li>o traffic and location data,</li> <li>o itemised billing,</li> <li>o line identification services (eg caller ID and call return</li> <li>o directory listings.</li> </ul> </li> </ul>	<a href="#">What are PECR?</a>
<b>Direct Marketing</b>	Communication (by whatever means) of advertising or marketing material which is directed to particular individuals. Includes promoting aims and beliefs, e.g. Political campaigning or charities.	<a href="#">Direct marketing</a>
<b>Frequently used terms</b>	<ul style="list-style-type: none"> <li>• <b>service provider:</b> provides telephone or internet services;</li> <li>• <b>network provider:</b> provides the underlying network equipment;</li> <li>• <b>Corporate subscriber:</b> subscribers that are a corporate body with separate legal status. This includes companies, limited liability partnerships, Scottish partnerships, and some government bodies.</li> <li>• <b>Individual subscriber:</b> covers individual customers (including sole traders) and other organisations (eg other types of partnership).</li> <li>• <b>user:</b> any individual using the phone or internet connection.</li> </ul>	<a href="#">Definitions</a>
<b>Solicited marketing</b>	if someone specifically asks to send them some information, PECR does not restrict such marketing (although must still say who they are, display the number when making calls, and provide a contact address)	<a href="#">Solicited marketing</a>
<b>Unsolicited marketing</b>	any message that has not been specifically requested, even if the customer 'opted-in'.	<a href="#">Unsolicited marketing</a>



<p><b>Soft opt in</b></p>	<p>It only applies where a company can meet all three criteria:</p> <ul style="list-style-type: none"> <li>• The company have obtained the contact details for the recipient in the course of a sale, or the negotiations for the sale, of a product or service to that recipient.</li> <li>• The direct marketing material they are sending is only about their own similar products and services.</li> <li>• The recipient was given a simple means of opting out at time their details were initially collected and is given an opt out opportunity at time of each subsequent communication.</li> </ul> <p>Does not apply to prospective customers or new contacts (e.g. from bought-in lists). It does not apply to non-commercial promotions (e.g. charity fundraising or political campaigning).</p>	<p><a href="#">Soft opt-in</a></p>
---------------------------	---	------------------------------------

### ELECTRONIC MARKETING BY REGULATION

<p><b>19 – Automated Calls</b></p>	<p><b>Individual &amp; Corporate subscribers:</b> Automated marketing calls cannot be made without prior consent.</p> <p><b>The caller must:</b></p> <ul style="list-style-type: none"> <li>- Say who is calling.</li> <li>- Allow the number to be displayed.</li> <li>- Provide contact details or a Freephone number if asked.</li> </ul>	<p><a href="#">What are the rules on automated calls?</a></p>
<p><b>20 – Faxes</b></p>	<p><b>Individual subscribers</b> - Marketing faxes cannot be sent to individual subscribers without prior consent.</p> <p><b>Corporate subscribers</b> - Marketing faxes cannot be sent to corporate subscribers registered with the Fax Preference service. Or those who have previously asked not to receive them.</p>	<p><a href="#">What are the rules on sending faxes?</a></p>

<p><b>21 – ‘Live’ Telephone calls</b></p>	<p><b>Individual subscribers</b> - Live marketing calls cannot be made to individual subscribers that:</p> <ul style="list-style-type: none"> <li>- Are registered with the Telephone Preference Service (TPS)</li> <li>- Have previously asked not to be called.</li> </ul> <p><b>Corporate subscribers</b> - Live marketing calls cannot be made to corporate subscribers that:</p> <ul style="list-style-type: none"> <li>- Are registered with the Corporate Telephone Preference Service (CTPS).</li> <li>- Have previously asked not be called.</li> </ul> <p><b>The caller must:</b></p> <ul style="list-style-type: none"> <li>- Say who is calling.</li> <li>- Allow the number to be displayed.</li> <li>- Provide contact details or a Freephone number if asked.</li> </ul>	<p><a href="#">When can we make marketing calls to individuals?</a></p> <p><a href="#">When can we make marketing calls to businesses?</a></p>
<p><b>21A – claims management calls</b></p>	<p><b>Individual &amp; Corporate subscribers:</b> Automated marketing calls cannot be made without prior consent.</p> <p><b>The caller must:</b></p> <ul style="list-style-type: none"> <li>- Say who is calling.</li> <li>- Allow the number to be displayed.</li> <li>- Provide contact details or a Freephone number if asked.</li> </ul>	<p>-</p>
<p><b>21B - pension scheme calls</b></p>	<p><b>Individual subscriber</b> - Callers must:</p> <ul style="list-style-type: none"> <li>- Be trustee or manager of scheme authorised by the Financial Conduct Authority.</li> <li>- Must have consent or meet strict criteria.</li> <li>- Must allow number to be displayed.</li> <li>- Say who is calling.</li> <li>- Provide contact details or a Freephone number if asked.</li> </ul> <p>Note - If a caller is targeting an individual at a corporate subscriber the above rules apply.</p>	<p>-</p>

<p><b>22 – Electronic Mail – Text messages, e- mails etc</b></p>	<p><b>Individual subscriber</b> - Marketing electronic mail (emails &amp; text) cannot be sent to an individual without prior consent.</p> <p>Unless the sender can demonstrate a <b>soft opt in</b>. This only applies when <b>ALL</b> of the following can be demonstrated:</p> <ul style="list-style-type: none"><li>- The sender <b>obtained the contact details in the course of a sale, or the negotiation for the sale of a product or service.</b></li><li>- The marketing material is only about their <b>own similar products or services.</b></li><li>- The recipient was given a <b>simple means of opting out at the time their details were collected</b> and is given an opt out opportunity in each subsequent communication.</li></ul> <p><b>Corporate subscribers</b> - The regulation does not apply unless the corporate subscriber is an individual (i.e. sole trader).</p> <p><b>The sender must:</b></p> <ul style="list-style-type: none"><li>- Not disguise or conceal their identity.</li><li>- Provide a valid contact address or Freephone number to opt out.</li></ul>	<p><a href="#">What are the rules on electronic mail marketing?</a></p> <p><a href="#">What is a 'soft opt-in'?</a></p>
--	---	---

**PECR & GDPR LINK BY REGULATION**

<p align="center"><b>Emailing company email address that does not identify any individual e.g. info@companyname</b></p>	<p><b>Regulation 22</b> does NOT apply to this type of email address (<b>Corporate subscriber</b>).</p> <p>However still must say who you are and give a valid address for the recipients to unsubscribe from your emails (<b>regulation 23</b>).</p> <p>It is also good practice to maintain a suppression (do not email or text) list for the future.</p>	<p><b>Lawful basis:</b> If this is the only information held: - consent not required. - nor any other GDPR lawful basis</p>
<p align="center"><b>Emailing corporate subscriber email address which identifies an individual e.g. EmployeeName@companyname</b></p>	<p><b>Regulation 22</b> does NOT apply to this type of email address (<b>corporate subscriber</b>).</p> <p>However still must say who you are and give a valid address for the recipients to unsubscribe (<b>regulation 23</b>).</p> <p>GDPR does apply (as email address includes individual's name) – if considering legitimate interests, must conduct balancing test to check whether marketing would fall within reasonable expectations of individual and that the processing would not prejudice their rights.</p> <p>Also need to provide '<b>right be informed</b>' information. NB if individual objects to future marketing, must then suppress their details.</p>	<p><b>Lawful basis</b> Consent not necessarily required. Could consider legitimate interests instead.</p>

<p><b>22 - Emailing sole traders and certain types of partnership (see definitions guidance on individual/corporate subscribers)</b></p>	<p>Treated as an <b>individual subscriber</b> under PECR and GDPR rules</p> <p>Requires <b>consent (or the soft opt-in)</b> and should send '<b>right to be informed</b>' information.</p> <p>Also need to give a valid address for recipients to unsubscribe (<b>regulation 23</b>).</p> <p>If relying upon soft opt-in, appropriate GDPR lawful basis will be legitimate interests not consent, so will need to conduct LIA balancing test.</p> <p>NB if recipient objects to future marketing, must then suppress their details.</p>	<p><b>Lawful basis:</b> Need consent if new contact</p> <p>If previous contact, need consent or could consider whether can meet requirements of soft opt-in</p>
<p><b>19 - Automated Calls</b></p>	<p>PECR Regulation 19 – Say who is calling, allow number to be displayed and provide contact details or Freephone number</p>	<p><b>Lawful basis:</b> Need consent</p>
<p><b>21 A - All claims management calls</b></p>	<p>PECR Regulation 21A (marketing calls about claims management services). Say who is calling, allow number to be displayed and provide contact detail or Freephone number</p>	<p><b>Lawful basis:</b> Need consent</p>
<p><b>21 B - Live Pension Calls</b></p>	<p>PECR Regulation 21B (marketing calls about pension schemes).</p> <p>Must say who is calling and provide contact details or Freephone number.</p> <p>Reg refers to calls to an individual not an 'individual subscriber'. If targeting individual on their corporate phone number on their corporate phone number, <b>individual rules apply</b>.</p>	<p><b>Lawful basis:</b> Consent</p> <p>Unless very strict criteria set by FCA can be met.</p>

<p><b>Live Calls</b></p>	<p>If relying upon legitimate interests, will still need to conduct legitimate interests balancing test.</p> <p>Must say who is calling (e.g. the name of your organisation), must allow your number (or an alternative contact number) to be displayed to the person receiving the call; and must provide your contact details or a Freephone</p>	<p><b>Lawful basis:</b> could consider legitimate interests basis.</p> <p><b>Unless:</b> number is listed on TPS, CTPS, or own suppression list of people who have objected to marketing previously.</p>
<p><b>Faxing a corporate body:</b></p>	<p>Also need to include your name and contact address or Freephone number on all B2B direct marketing faxes.</p>	<p><b>Lawful basis:</b> Could consider legitimate interests</p> <p><b>Unless:</b> number is listed on the Fax Preference Service or organisation's own suppression list</p>
<p><b>20 - Faxing sole traders and certain partnerships</b></p>	<p>PECR treats these as individual subscribers</p>	<p><b>Lawful basis:</b> Consent <b>See definitions</b> (above)</p>

## COOKIES AND RELATED TECHNOLOGIES

<p><b>Cookies and related technologies definitions</b></p>	<p>Cookies are small pieces of information, normally consisting of just letters and numbers, which online services provide when users visit them. Related technologies could also include, HTML5 local storage, Local Shared Objects and fingerprinting techniques.</p>	<p><a href="#">What are cookies and similar technologies</a></p>
<p><b>Frequently used terms</b></p>	<p><b>Session cookies</b> expire after the user closes their browser.  <b>Persistent Cookies</b> are saved on the users device between sessions.  <b>Terminal equipment</b> refers to the device a cookie is placed on – typically a computer or mobile device, but also other devices.</p>	<p><a href="#">Frequently used terms</a></p>
<p><b>PECR requirements for cookies</b></p>	<p><b>Give 'clear and comprehensive information'</b>  PECR does not define this term, however Article 5(3) of the ePrivacy Directive says: clear and comprehensive information should be provided 'in accordance with' data protection law'.</p> <p><b>Obtain consent</b>  GDPR standard of consent applies meaning consent:  -is requested using clear and plain language  -must be clearly distinguished from other matters  -can be withdrawn at any time  -does not use pre-ticked boxes</p>	<p><a href="#">Clear and comprehensive</a></p> <p><a href="#">Obtain consent</a></p>
<p><b>The strictly necessary, and communications exemptions</b></p>	<p>The above requirements do not apply if either exemption can be used:</p> <ul style="list-style-type: none"> <li>• the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or</li> <li>• the cookie is strictly necessary to provide an 'information society service' (e.g. a service over the internet) requested by the subscriber or user. Note that it must be essential to fulfil their request – cookies that are helpful or convenient but not essential, or that are only essential for your own purposes, will still require consent.</li> </ul> <p>Our guidance states that it is still good practice to provide clear information about all cookies, even those covered by an exemption.</p>	<p><a href="#">Transmission of communication</a></p> <p><a href="#">Strictly necessary</a></p>

**POLITICAL CAMPAIGNING AND PECR**

<p><b>Includes fundraising, campaigning and the promotion of the aims and ideals of an organisation</b></p>	<p>Most political messaging directed to particular individuals is considered to be direct marketing. Whilst genuine service communications and market research don't fall under marketing rules, PECR will apply if they are used to send political campaigning messages urging people to support a campaign, candidate, fund raise or encouraging individuals to take some form of direct action.</p>	<p><a href="#"><u>Political campaigning – direct marketing</u></a></p>
<p><b>Political parties and MPs need to follow PECR regulations in full</b></p>	<p>They cannot rely upon the soft opt-in because this option only applies if an organisation has engaged in the commercial marketing of products and services. Therefore, can only send a campaigning email if person has specifically consented to receiving campaigning emails from them.</p>	<p><a href="#"><u>What is 'advertising or marketing material'?</u></a></p>
<p><b>Viral marketing</b></p>	<p>Encouraging people to forward a message onto friends is likely to breach PECR as cannot obtain consent as have no direct contact with end recipient of message.</p>	<p><a href="#"><u>Can we carry out viral marketing?</u></a></p>
<p><b>Right to object to (political) campaigning</b></p>	<p>Individuals have a right to object to all campaigning messages sent by electronic means. Electoral law still allows political parties and candidates to send one 'election address' by Freepost - this is not considered direct marketing and so individuals cannot opt out of it, but as it is sent by post, PECR would not apply anyway.</p>	<p><a href="#"><u>How does the right to object apply?</u></a></p>
<p><b>Market research</b></p>	<p>PECR does not apply if there is no direct marketing intention, e.g. Research for product development or policies.</p> <p>If the purpose is to 'sell' under market research disguise (<b>'sugging'</b>), PECR applies, also could be GDPR infringement</p>	<p><a href="#"><u>When does opinion research become direct marketing?</u></a></p>



## **Privacy and Electronic Communications Regulations**

### **What are the Privacy and Electronic Communication Regulations?**

Legislation that sits alongside GDPR & DPA18 –

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

#### *Questions to ask trainees*

- *What do you think we get the most queries on re PECR?*
- *Have you listened to any helpline calls that stand out?*

### **Key definitions of PECR**

See [departmental handout](#)

### **What is marketing?**

Definition in handout – Explain that this is a questions that we are often asked by data controllers.

Examples:

- Promotional material from charities
- Reminder e-mails sent to customers / potential customers
- Political campaigning

### **Email and text marketing.**

Highlight the key difference between individual subscriber and corporate subscriber.

### **Individual subscribers –**

You must not send marketing emails or texts to individuals subscribers without specific consent. There is a limited exception for your own previous customers, often called the 'soft opt-in'.

Three parts to the soft opt in:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;
- they are only marketing their own similar products or services; and
- they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.
- This can be split further into five points a data controller must satisfy to rely on the soft opt-in:
  - o You obtained the contact details;
  - o In the course of a sale or negotiation of a sale of a product or service;
  - o Your similar products and services are being marketed;
  - o Opportunity to refuse or opt-out given when you collected the details; and
  - o Opportunity to refuse or opt-out given in every communication.

**Corporate subscribers (B2B)** - These rules on consent, the soft opt-in and the right to opt out do not apply to electronic marketing messages sent to 'corporate subscribers' which means companies and other corporate bodies.

Corporate subscribers do not include sole traders and some partnerships who instead have the same protection as individual customers.

Individual employees have rights under the GDPR to object. E.g. ICO e-mail addresses.

### **Telephone Marketing.**

**Live marketing calls** - you must not make unsolicited live calls:

- to anyone who has told you they don't want your calls;
- to any number registered with the TPS or CTPS, unless the person has specifically consented to your calls – even if they are an existing customer (unless the call is in relation to pension schemes and you meet a strict criteria, see below);
- for the purpose of claims management services, unless the person has specifically consented to your calls; or

- in relation to pension schemes unless you are a trustee or manager of a pension scheme or a firm authorised by the Financial Conduct Authority, and the person you are calling has specifically consented to your calls or your relationship with the individual meets a strict criteria.

Automated calls – Should not be made without prior consent in all cases. This consent must specifically cover automated calls.

Ask re TPS, demonstrate website. Background on pension schemes and claims management.

### **Marketing calls to business – Any guesses?**

Rules are the same as to individuals, so calls can be made with prior consent, or to businesses not on the CTPS/not making calls re claims management services.

B2B calls generally need to be screened against TPS & CTPS as sole traders register with the TPS.

### **DPA/GDPR compliance.**

Ask the trainees where do they think the main crossover will come? **Hint** - think about individual rights.

- Definition of consent
- Right to object (absolute for direct marketing)
- Soft opt in – can cause confusion among both DS & DC's. Go through this.
- Aspects of PECR will apply regardless of whether personal data is being processed e.g. Cookies (will be covered shortly)

### **ICO action & reporting tool.**

Lots of ICO enforcement action relates to PECR breaches, nuisance calls etc. Have a look at Action We've Taken PECR breaches. Important aspect of ICO enforcement, any reasons why? Reputation?

Reporting tool – explain that this will be mostly used by Public Advice but this is where customers can report nuisance calls. Take through the reporting tool.

### **Other elements of PECR (Cookies, location data, CLI and itemised billing).**

Other elements are not particularly common. Cookies will come up however. Recent ICO guidance published on Cookies. Cookies are often a point of contention for DC's, however rules are fairly simple:

*You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent. Consent must be actively and clearly given.*

*There is an exception for cookies that are essential to provide an online service at someone's request (eg to remember what's in their online basket, or to ensure security in online banking).*

*The same rules also apply if you use any other type of technology to store or gain access to information on someone's device.*

Highlight new ICO cookies guidance – covers all of the considerations in lots of detail. Highlight other technologies e.g. tracking pixels.

Talk through the remaining 'other elements' (Security of services, Security breaches, Traffic data, Location data, Itemised bills, CLI, Directories) in particular highlighting the 'in brief' section on the respective website pages as these effectively summarise the rules on each part.

### **Other regulators.**

Telephone Preference Service – Highlight website

Ofcom – Silent / abandoned calls

Phone Paid Services Authority – Phone bill charges

Action Fraud

### **Introduction to relevant guidance.**

Knowledge Builder – Direct marketing & PECR

PECR Desk Aid

Electronic marketing guidance

Draft direct marketing code

SME Hub on Marketing

## **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)**

### **Key definitions**

<b>Subscriber</b>	This means the person who pays the bill for the use of the line (that is, the person legally responsible for the charges)
<b>Individual Subscriber</b>	This means a residential subscriber, a sole trader or a non-limited liability partnership in England, Wales and Northern Ireland.
<b>Corporate Subscriber</b>	This includes corporate bodies such as a limited company in the UK, a limited liability partnership in England, Wales and Northern Ireland or any partnership in Scotland. It also includes schools, government departments and agencies, hospitals and other public bodies, for example, the Information Commissioner's Office.
<b>User</b>	Means any individual using a public electronic communications service (e.g. using the phone or internet connection). For example, the individual subscriber to a mobile phone could be parent but the user their child.
<b>Service Provider</b>	Means someone who provides any service allowing members of the public to send electronic messages (providers of telephone or internet services).
<b>Direct Marketing (section 122 of DPA18)</b>	Means the communication by (whatever means) of advertising or marketing material which is directed to particular individuals.
<b>Consent</b>	Consent must be freely given, specific informed and There must be an indication signifying agreement. It must be unambiguous and involved a clear affirmative action.

<b>Regulation</b>	<b>Individual subscribers</b>	<b>Corporate subscribers</b>
<b>19 – Automated Calls</b>	<p>Do not make unsolicited automated marketing telephone calls without prior consent.</p> <p>Say who is calling, allow number to be displayed and provide contact details or Freephone number.</p>	<p>Do not make unsolicited automated marketing telephone calls without prior consent.</p> <p>Say who is calling, allow number to be displayed and provide contact details or Freephone number.</p>
<b>20 – Faxes</b>	<p>Do not send unsolicited marketing faxes to individual subscribers without prior consent</p>	<p>Do not send unsolicited marketing faxes to numbers which are registered with the FPS or where you have been asked not to.</p>
<b>21 – ‘Live’ Telephone calls</b>	<p>Do not make unsolicited marketing telephone calls to subscribers who are either: -</p> <p>Registered with the TPS or CTPS <b>or</b></p> <p>Have previously asked the company not to call them.</p> <p>Say who is calling and allow number to be displayed. Provide contact details or Freephone number if asked.</p>	<p>Do not make unsolicited marketing telephone calls to subscribers who are either: -</p> <p>Registered with the CTPS or TPS <b>or</b></p> <p>Have previously asked the company not to call them.</p> <p>Say who is calling and allow number to be displayed. Provide contact details or Freephone number if asked</p>
<b>21A – claims management calls</b>	<p>Do not make unsolicited marketing calls about claims management unless have consent.</p> <p>Say who is calling and allow number to be displayed. Provide contact details or Freephone number if asked.</p>	<p>Do not make unsolicited marketing calls about claims management unless have consent.</p> <p>Say who is calling and allow number to be displayed. Provide contact details or Freephone number if asked.</p>
<b>21B pension scheme calls</b>	<p>Must be trustee or manager of scheme or authorised by FCA. Must have either consent or meet strict criteria.</p>	<p>Refers to calls to an individual not an ‘individual subscriber’. If targeting individual on their corporate phone number then individual rules apply.</p>

	<p>Allow number to be displayed.</p> <p>Say who is calling and provide contact details or Freephone number if asked</p>	
<p><b>22 – Electronic Mail – Text messages, e-mails etc</b></p>	<p>Do not send unsolicited marketing material by electronic mail to individual subscribers without prior consent.</p> <p><b>Only</b> exception to this rule is the '<b>soft opt in</b>'.</p> <p>It only applies where a company can meet <b>all</b> three criteria</p> <ol style="list-style-type: none"> <li>1. The company have obtained the contact details for the recipient <b>in the course of a sale, or the negotiations for the sale, of a product or service to that recipient.</b></li> <li>2. The direct marketing material they are sending is only about <b>their own similar products and services.</b></li> <li>3. The recipient was given a simple means of opting out at time their details were initially collected and is given an <b>opt out</b> opportunity at time of each subsequent communication.</li> </ol> <p>Must not disguise or conceal identity and must provide a valid contact address or Freephone number for individuals to opt out or unsubscribe</p>	<p>Reg 22 does not apply.</p> <p>No prior consent requirement for sending electronic mail marketing to corporate subscribers. (Remember sole traders &amp; some partnerships are classed as individual subscribers)</p> <p>However, <b>do</b> need to identify yourselves and provide valid address for opt outs in communications.</p> <p><b>Note: Check no Article 21(2) right applies (right to object to direct marketing) where corporate subscriber email address is personal data e.g. Joe.bloggs@ico.gsi.gov.uk</b></p>

## ePrivacy Directive

### What is the ePrivacy Directive?

The process for adopting a new ePrivacy Regulation (ePR) is now underway. This will eventually replace the ePrivacy Directive, (which implemented existing ePrivacy rules, including on marketing and cookies, in the UK). Whilst the ePR won't directly apply to the UK, it is likely to have implications for British businesses, particularly those with customers in the EU.

The EU Commission published a proposed draft ePrivacy Regulation in January 2017. Negotiations within the EU have continued up until February 2021, where a draft by the Council of the EU was published. Trilogue negotiations will follow this, but a final draft isn't expected to enter into force until 2023. There is also the potential for a 24 month transition period, meaning that final ePR may not become EU law until 2025.

### Status of ePrivacy Directive & Implications

The ICO is monitoring the situation. We'll also be discussing any wider implications in relation to the ePR with the UK government.

Until the ePR is agreed by the European Council, the content is subject to debate and amendment. We cannot give any detailed lines or guidance until the final text is agreed and adopted. However, we intend to keep our [Electronic Marketing guidance](#) updated with information about the progress of the ePR and guidance plans, and that site should always be checked for the latest information.

## Direct Marketing Code

The Information Commissioner is required under the Data Protection Act 2018 to produce a direct marketing code of practice to provide practical guidance and promote good practice in regard to processing for direct marketing purposes. A draft code was issued for public consultation which closed in March 2020 shortly before the start of the Covid-19 pandemic and the work was subsequently paused. The work on the code recommenced in mid-2021, and will be accessible via [this page](#) once complete.



## PECR also covers...

### Traffic Data

Information about the timing and routing of a telephone call.

### Location Data

Information collected by a network or service about where the user's phone or other device is or was located.

### Itemised Bills

The right to receive bills that are not itemised, telephone service providers must comply with that request.

### Line identification

Service providers must:

- allow callers to withhold their number;
- allow called subscribers to prevent the caller's number being displayed;
- provide an anonymous-call rejection service;
- allow called subscribers to withhold their number; and
- provide information to the public about CLI services.

### Directories

if you want to compile a directory, you must:

- tell individual subscribers;
- give them the chance to choose whether to be included;
- get their express consent for reverse searches; and
- correct or withdraw entries on request.

You cannot charge for opt-outs or corrections.

## Useful Links

### **Guide to PECR**

<https://ico.org.uk/for-organisations/guide-to-pecr/>

### **Knowledge Builder – Direct Marketing & PECR**

[TGrp ICO Knowledge Centre Corporate Affairs and Governance - Direct Marketing & PECR - All Pages \(sharepoint.com\)](#)

### **Direct Marketing guide**

<https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf>

## **Draft Direct Marketing code**

[Direct marketing code of practice Draft code for consultation \(ico.org.uk\)](#)

## **B2B marketing**

[Business-to-business marketing | ICO](#)

## **SME Hub – PECR basics blog**

[Don't get caught out by PECR | ICO](#)

## **SME Hub – Marketing and consent**

[Marketing and consent | ICO](#)

## **Cookies and similar technologies**

<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>

## **Your data matters guidance on nuisance calls**

<https://ico.org.uk/your-data-matters/nuisance-calls/>

## **Your data matters guidance on spam emails**

<https://ico.org.uk/your-data-matters/online/spam-emails/>

## **Your data matters guidance on spam texts**

<https://ico.org.uk/your-data-matters/texts/>

## **Your data matters guidance on cookies**

<https://ico.org.uk/your-data-matters/online/cookies/>

## **Other Regulators/Bodies**

### **Telephone Preference Service**

If you register your number with the TPS and you continue to receive nuisance live marketing calls 28 days after registering, you can complain either directly to the TPS or you can report your concerns to us.

[Telephone Preference Service \(tpsonline.org.uk\)](#)

### **Ofcom**

Silent or abandoned calls should be reported to Ofcom.

<https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/problems/tackling-nuisance-calls-and-messages/abandoned-and-silent-calls>

### **Phone Paid Services Authority**

The Phone-paid Services Authority (PSA) regulates products or services that are charged to users' phone bills or pre-pay accounts. You can contact them to report these calls or to access details of the premium rate number ranges the PSA regulates.

<https://psauthority.org.uk/>

### **Action Fraud**

Fraud and scam calls, messages and emails should be reported to Action Fraud.

<https://www.actionfraud.police.uk/>

## The Network and Information Systems Regulations (NIS) quiz

The aim of this quiz is to help staff understand the NIS regulations. All the answers to these questions can be found on our website, specifically, [in the Guide to NIS](#). Staff can point customers to these areas when they are in contact with them.

Question	Answer	Website section
<b>NIS</b>		
What is the purpose of NIS?	NIS is intended to establish a common level of security for network and information systems.	For organisations > The Guide to NIS > What is NIS?
Which organisations are covered by NIS?	NIS applies to two groups of organisations: 'operators of essential services' (OES) and 'relevant digital service providers' (RDSPs).	For organisations > The Guide to NIS > What is NIS?
What type of incidents does NIS apply to?	NIS applies to cyberincidents but also 'non-cyber' ones such as power supplies or natural disasters.	For organisations > The Guide to NIS > What is NIS?
What are the three conditions to be considered a RDSP?	The organisation needs to provide one of more of the following: an online search engine, an online marketplace and a cloud computing service. It also needs to have its head officer in the UK (or have a nominated UK representative) and have more than 50 staff and a turnover or balance sheet of more than €10 million.	For organisations > The Guide to NIS > What is NIS?
What is the definition of a 'network and information systems'? How does it link NIS with GDPR?	Regulation 1 of NIS defines a 'network and information system' as:  (a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under point (a) or (b) for the purposes of their operation, use, protection and maintenance; Digital data can be personal data.	For organisations > The Guide to NIS > Key concepts and definitions
What is the definition of 'security of network	Regulation 1 of NIS defines it as: 'the ability of network and information systems to resist,	For organisations > The Guide to NIS > Key concepts and definitions

and information systems’?	at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.’	
What is the definition of an OES?	An operator of essential services. Essential service is a service which is essential for the maintenance of critical societal or economic activities (eg. water, health services, energy, transport)	For organisations > The Guide to NIS > Key concepts and definitions
What is the role of the ICO?	<p>The ICO is the ‘competent authority’ for RDSPs for the purposes of NIS (but will also be the competent authority for both OES and RDSPs if they process personal data for the purposes of GDPR).</p> <p>In that capacity, we are required to:</p> <ul style="list-style-type: none"> <li>-review the application of NIS on RDSPs;</li> <li>-prepare and publish guidance for RDSPs;</li> <li>-consult and co-operate with other relevant agencies, such as law enforcement, other competent authorities, and the NCSC; and</li> <li>-undertake enforcement action, where appropriate.</li> </ul>	For organisations > The Guide to NIS > Key concepts and definitions + For organisations > The Guide to NIS > What is NIS?
What is the SPOC and the CSIRT?	<p>‘Single Point of Contact’, their role is to coordinate with other Competent Authorities in different Member States for cross-border co-operation. They report to a European-level ‘Cooperation Group’ as well as the EU Commission. The NCSC is the UK SPOC.</p> <p>‘Computer security incident response team’, their role is to monitor and respond to incidents. It also has other functions such as providing warnings and disseminate information about risks and incidents. The NCSC is the UK CSIRT.</p>	For organisations > The Guide to NIS > Key concepts and definitions

**Digital Service Providers**

Does NIS cover an organisation which provides a digital service to their employees?	No, it would only cover organisations that provide a digital service to external customers.	For organisations > The Guide to NIS > Digital service providers
What is the definition of an online search engine?	'a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found' – a web search operator (however most well-known ones such as Google aren't based in the UK so they aren't covered by NIS)	For organisations > The Guide to NIS > Digital service providers
What is the definition of an online marketplace?	'a digital service that allows consumers and/or traders [...] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace' Not all these platforms are considered marketplaces (eg. Price comparison websites, classified ads, ...)	For organisations > The Guide to NIS > Digital service providers
What is the definition of a cloud computing service?	'A digital service that enables access to a scalable and elastic pool of shareable computing resources.' 3 main categories of cloud computing services (SaaS, PaaS, IaaS)	For organisations > The Guide to NIS > Digital service providers
Does an RDSP need to register with the ICO?	<p>'Yes. If you are an RDSP, Regulation 14 of NIS requires you to register with the ICO by 1 November 2018. Unlike registration under data protection law, there is no fee required for NIS. You should register with the ICO by emailing <a href="mailto:dataprotectionfee@ico.org.uk">dataprotectionfee@ico.org.uk</a> with the subject line 'RDSP registration details', and include the following in your email:</p> <p>the name of your organisation;  the name of your service;  the address of your head office, or that of your nominated representative; and</p>	<p>For organisations &gt; The Guide to NIS &gt; Digital service providers</p> <p><a href="#">(List of RDSP registered with us available on DP Fees Sharepoint)</a></p>

	<p>up-to-date contact details, including the name of a nominated individual who we can contact about NIS related matters if we need to, their email address and their telephone number.</p> <p>You can also provide this information via our helpline on 0303 123 1113.</p> <p>You also need to notify us of any change to these details as soon as possible, and no later than three months after the change taking place.</p> <p>If you become an RDSP after 1 November 2018, you must notify us within three months.</p> <p>If you are also a data controller, you need to register with us separately to pay the data protection fee.'</p>	
<p>What are the security requirements?</p>	<p>RDSPs must 'identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems'</p>	<p>For organisations &gt; The Guide to NIS &gt; Security requirements</p>
<p>What should RDSPs take into account when considering their security measures?</p>	<p>They should take into account the security of their systems and facilities, their policies and procedures for incident handling, their business continuity management, their policies and procedures for monitoring, auditing and testing and their compliance with international standards.</p>	<p>For organisations &gt; The Guide to NIS &gt; Security requirements</p>
<p>What other security requirement apply to RDSPs?</p>	<p>They must have 'adequate' documentation available to demonstrate compliance with the security elements and must make it available to the ICO if necessary. The ICO can take enforcement action if it is not the case.</p>	<p>For organisations &gt; The Guide to NIS &gt; Security requirements</p>

What enforcement powers does the ICO have?	The ICO has a range of available enforcement actions, including information notices, enforcement notices, penalty notices and inspection powers.	For organisations > The Guide to NIS > Enforcement
<b>Incident reporting</b>		
What is the definition of an incident?	'Any event having an actual adverse effect on the security of network and information systems'	For organisations > The Guide to NIS > Incident reporting
What is the timeframe to report a NIS incident to the ICO?	A RDSPs is required to notify the ICO of any incident without undue delay and not later than 72 hours of becoming aware of it. An OES should notify the competent authority for their sector.	For organisations > The Guide to NIS > Incident reporting
What information must RDSPs provide to the ICO?	They must provide: <ul style="list-style-type: none"> <li>- the name of the organisation and types of digital services they provide</li> <li>- The time the incident occurred</li> <li>- The incident's duration</li> <li>- Information about the incident's nature and impact</li> <li>- Information about any cross-border impact</li> <li>- Any other information that may assist the ICO.</li> </ul> There is a NIS incident reporting form on the website.	For organisations > The Guide to NIS > Incident reporting
Should RDSPs report all incidents to the ICO?	They only need to notify the ICO if the incident has caused a 'substantial impact on the provision' of their digital services. To assess this, they should take into account the number of users affected by the incident, the duration of it, the geographical spread, the extent of the disruption, any impact on economic and societal activities, and whether one of the situations specified in Article 4 of the DSP has taken place. They are only required to notify the ICO if the threshold is met. However, they are encouraged to provide voluntary notification reports of other incidents.	For organisations > The Guide to NIS > Incident reporting



Do they need to notify any other organisation?	The ICO is required to share incident notifications with NCSC but the organisation can voluntarily report them, especially if they may need their support to manage the incident. They should also consider notifying the National Crime Agency or Action Fraud if applicable.	For organisations > The Guide to NIS > Incident reporting
Do they need to notify the public?	The ICO may decide to inform the public if necessary (public interest) but will consult the organisation first.	For organisations > The Guide to NIS > Incident reporting
<b>GDPR and NIS</b>		
What are the main differences between GDPR and NIS?	NIS covers digital data (which may include personal data but not only). Digital data however does not include manual data (which may be covered by GDPR if it forms or is intended to form part of a filing system).	For organisations > The Guide to NIS > GDPR and NIS
What is the difference between a NIS incident and a GDPR personal data breach?	A NIS incident relates to computer systems and digital data stored and processed within them. This can include personal data but not necessarily. A NIS incident may lead to a personal data breach.	For organisations > The Guide to NIS > GDPR and NIS
Who do organisations report to?	It depends on their circumstances. If they are dealing with a NIS incident which is also a personal data breach, then they should report to both their competent authority under NIS (the ICO if they are an RDSP) and the ICO (under GDPR). Both notifications should be made without undue delay and within 72 hours, where feasible.	For organisations > The Guide to NIS > GDPR and NIS
Can organisations be fined twice (under NIS and GDPR)?	GDPR and NIS are separate laws, so an organisation may be subject to regulatory action under both. However, it would relate to different aspects of the incident and the potential infringements of the specific laws in question. Where the ICO is not the competent authority under NIS, we will work closely with the relevant competent authority to maintain a common approach.	For organisations > The Guide to NIS > GDPR and NIS

## Website Quiz - Answers

The following questions are all based around the information available on our website.

When answering the questions you should provide a brief summary of your answer and a link to where you found the answer on our website. For example, question one asks how an individual can obtain a copy of their personal information. Your answer to this would be: By making a subject access request (SAR) <https://ico.org.uk/your-data-matters/your-right-of-access/>.

## Website Quiz - Answers

The following questions are all based around the information available on our website.

When answering the questions you should provide a brief summary of your answer and a link to where you found the answer on our website. For example, question one asks how an individual can obtain a copy of their personal information. Your answer to this would be: By making a subject access request (SAR) <https://ico.org.uk/your-data-matters/your-right-of-access/>.

## Your Data Matters

- 1 How can an individual obtain a copy of their personal information? **Individuals can obtain their personal data by making a subject access request (SAR) - <https://ico.org.uk/your-data-matters/your-right-of-access/>**
- 2 How can an individual obtain a copy of their credit file and is there any differences to this and the answer to question 1? **Individuals can obtain a copy of their credit file in the same way they make a SAR – most CRAs have forms to use <https://ico.org.uk/your-data-matters/credit/>**
- 3 What should individuals ask themselves when using CCTV on their property? **Individuals should ask themselves whether they need to use intrusive measures such as CCTV for their purposes <https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/>**
- 4 What can an individual do about internet search results which may affect their privacy? **Individuals can ask search engines to remove results containing personal data – this is not an**

**absolute right** <https://ico.org.uk/your-data-matters/online/internet-search-results/>

- 5 What must charities do if they want to share personal information with other charities? **Charities need to inform individuals of the other charities who they will be sharing data with** <https://ico.org.uk/your-data-matters/charity-fundraising-practices/>
- 6 Can an individual report nuisance calls to us and, if so, how? **Individuals can report nuisance calls to us using our nuisance call reporting tool** <https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/>

## SME Web Hub

- 1 What kind of organisations should use our SME Web Hub for advice and guidance?  
**The SME Web Hub is for all small organisations, including small to medium-sized enterprises, small business, sole traders, small charities, group and clubs, and small start-ups** <https://ico.org.uk/for-organisations/sme-web-hub/>
- 2 Where can an SME find our Privacy Notice template?  
**SMEs can find the privacy notice template in the 'Make your own privacy notice' section of SME web hub** <https://ico.org.uk/for-organisations/make-your-own-privacy-notice/>
- 3 Do SMEs need to pay the Data protection fee?  
**All SMEs will need to pay the Data protection fee unless they are exempt** <https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/data-protection-fee-what-you-need-to-do/>
- 4 What are the seven steps an SME should take assessing risk in a personal data breach? **1. Check if personal data is involved 2. Establish what personal data has been breached 3. Consider who might have the personal data 4. Work out how many people might be affected 5. Consider how seriously it will affect people 6. Document everything else you know about the breach 7. Assess the risk** <https://ico.org.uk/for-organisations/sme-web-hub/understanding-and-assessing-risk-in-personal-data-breaches/>
- 5 Should an SME keep personal data they don't need 'just in case'?  
**No, data protection legislation says organisations shouldn't keep personal information any longer than they need it**

<https://ico.org.uk/for-organisations/sme-web-hub/common-data-protection-mistakes-and-how-to-fix-them/>

- 6 Where could an SME find the rules on Marketing and consent?  
**An SME should read our 'Don't get caught out by PECR' blog under the 'find the right resource' section**

<https://ico.org.uk/for-organisations/sme-web-hub/find-the-right-resource/>

## **For organisations**

### Guide to the GDPR

1. Where can organisations find our guide to the GDPR?  
**Organisations can find our guide to the GDPR in the "for organisations" section of the website, in the list of guides to the legislation - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>**
2. How is personal data defined? **Personal data is defined as information that relates to an identified or identifiable individual - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>**
3. Where can organisations find a checklist to help them determine whether they are a controller or processor? **Organisations can find a checklist to determine whether they are a controller or processor in the section of the Guide to the GDPR for controllers and processors <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/>**
4. What lawful bases are available to organisations? **The six lawful bases are consent, contract, public task, vital interests, legal obligation and legitimate interests - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>**
5. If an organisation needs to consult with us about their Data Protection Impact Assessment, how can they do so? **Organisations that need to consult with us about their DPIA can do so by emailing [DPIAconsultation@ico.org.uk](mailto:DPIAconsultation@ico.org.uk) - <https://ico.org.uk/for->**

[organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

6. What is an organisation required to do to process personal data securely? **Organisations must take appropriate technical and organisational measures to ensure the confidentiality, integrity and availability of personal data -** <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>
7. Where can an organisation find the list of exemptions available to them? **Organisations can find a list of the exemptions to the GDPR found in the DPA 2018, and what each exemption applies to, on our page for exemptions in our guide to the GDPR** <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>

### Registration

1. Where do organisations need to go on the website to register with us? **Organisations need to go to our registration page, found by pressing the button that says "pay fee, renew fee or register a DPO" on the for organisations section of the website** <https://ico.org.uk/for-organisations/data-protection-fee/>
2. Where can organisations take a self-assessment to find out if they need to register with us? **Organisations can find a self-assessment to determine whether they need to register with us on our registration page** <https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/>
3. Is the data protection register published anywhere? **The data protection register is published on our website – individuals and organisations can search it using our search function or download the full register** <https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/>

### PECR

1. Where can organisations find our guidance for electronic communications and marketing? **Organisations can find our guidance for PECR in the guides to the legislation, on the page titled "Electronic Communications and Marketing"** <https://ico.org.uk/for-organisations/guide-to-pecr/>
2. What is the definition of 'direct marketing'? **Direct marketing is defined as "the communication (by whatever means) of advertising or marketing material which is directed to**

**particular individuals”** <https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/>

3. Where can organisations find the rules for telephone marketing? **Organisations can find the rules for telephone marketing in the Electronic Communications and Marketing guidance, on the page for telephone marketing** <https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/telephone-marketing/>
4. What is the general rule for marketing by electronic mail? Are there any exceptions? **The general rule for marketing by electronic marketing is that the organisation must have the consent of the individual. The only exception is the soft opt-in.** <https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/>

### Freedom of Information

1. Where can public authorities find our guidance on Freedom of Information? **PAs can find our guidance on FOI in our guides to the legislation, in the section titled “Guide to Freedom of Information”** <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>
2. Where can public authorities find our guidance on exemptions under FOI? **PAs can find our guidance on the exemptions under FOI on the page called “refusing a request” in our FOI guidance** <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/>
3. Where can a list of our decision notices be found? **A list of our DNs can be found on the “Action We’ve Taken” page** <https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&profile=decisions&query>

### General

1. Where can an SME find information on steps to take when installing CCTV? **SMEs can find a step-by-step guide on Installing CCTV in the SME web hub** <https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/installing-cctv-things-you-need-to-do-first/>
2. Where can organisations find our guidance on data protection and Brexit? **Organisations can find our guidance on data protection and Brexit in our guides to the legislation** <https://ico.org.uk/for-organisations/data-protection-and-brexit/>
3. Where can small business owners and sole traders find a self-assessment for data protection compliance? **Small business owners and sole traders can find a self-assessment for data**

**protection compliance in our list of resources on the for organisations page** <https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/>

4. Where our frequently asked questions for SMEs be found? **Our FAQs for SMEs can be found in our list of resources on the for organisations page** <https://ico.org.uk/for-organisations/business/sme-faqs/>
5. Where can a list of our news items and blogs be found? **A list of our news items and blogs can be found on the home page, by pressing the “more news and blogs” button** <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/>
6. Where can a list of action we’ve taken be found? **A list of action we’ve taken can be found by pressing the “action we’ve taken” button on the top banner** <https://ico.org.uk/action-weve-taken/>
7. Where can our ICO and stakeholder consultations be found? **Our ICO and stakeholder consultations can be found on the “About the ICO” page, following the link for ICO and stakeholder consultations** <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/>
8. Where can our privacy notice be found? **Our privacy notice can be found at the bottom of the website page, following the link for “privacy notice”** <https://ico.org.uk/global/privacy-notice/>
9. Where can our copyright information be found? **Our copyright information can be found at the bottom of the website page, following the link for “copyright information”** <https://ico.org.uk/global/copyright-and-re-use-of-materials/>

## Template letter – reviewing officers final response

Updated Aug 2020

### For reviewing officer's to use – final response to case review

This letter could be used when you have already responded to a case review and follow up correspondence but there's no further action for you to take.

.....  
Dear xxx

Thank you for your letter of xxx concerning your complaint about xxx

I am sorry that you are disappointed with the service you have received from us and/or our decision making in this case.

You have however exhausted our case review process and we do not intend to consider the issues you have raised again.

If you would like to complain about the service you have received from us I would remind you that you may be able to complain to the Parliamentary and Health Service Ombudsman via your MP.

You also have the right to take your data protection concerns to court irrespective of the views we have provided. If this is something that you are interested in pursuing then we would advise you to seek independent legal advice.

I am sorry that we cannot be of any further assistance. Your case will remain closed and we do not intend to enter into further correspondence about this matter.

Yours sincerely

Name of reviewing officer  
Job title  
Information Commissioner's Office  
Direct dial telephone number

Please consider the environment before printing this email

For information about what we do with personal data see our [privacy notice](#)



## Template letter - case change final response

Updated March 2022

### To DS - final case change

This letter could be used when you have already responded to a DS' follow up correspondence and there's no further action for you to take.

.....

Dear xxx

Thank you for your letter of xxx about xxx

I understand that you remain concerned about the processing of personal data by [insert DC name] and you would like us to look into this matter further.

### What we do

Under data protection legislation, our obligation is to investigate a complaint about the handling of your personal data to an appropriate extent, and inform you of the outcome. Part of this process includes us considering whether further action is necessary or appropriate, in line with our [Regulatory Action Policy](#).

### Our view of your complaint

In this case, we do not consider that it is appropriate or necessary to pursue further action with [insert DC name] and/or we have provided [insert DC name] with advice about improving their wider information rights practices. We are satisfied they understand what we require them to do to put things right.

We have now provided you with our outcome and do not intend to take any further action. If you remain dissatisfied with how we have handled your complaint, you can complain to us within the next three months. You would need to complete the form on our website <https://ico.org.uk/make-a-complaint/complaints-and-compliments-about-us/>.

Yours sincerely

Name of case officer

Job title  
Information Commissioner's Office  
Direct dial telephone number

# **Can my neighbour operate CCTV on their property?**

## **Yes they can.**

However if your neighbour is capturing images outside of their property boundary or if they are operating a business from their property this may make them a data controller for the purposes of the Data Protection Act 2018 (DPA), and to ensure compliance with the DPA they would need to:

- Consider what area needs to be covered and what images will be captured,
- Safeguard any recorded images to enable usage by the police to investigate crimes,
- Install signage that indicates CCTV is operational in the area,
- Ensure the footage recorded is stored securely and only individuals access the data who need to,
- Be able to respond appropriately to a request for the footage from individuals who appear in it.

If your neighbour does not appear to have taken these steps it may be the case that

- images outside of their boundary are not being captured.
- your neighbour may not have their CCTV turned on or
- the cameras could be dummy cameras.

Further information on the DPA requirements can be found on our website at [www.ico.org.uk](http://www.ico.org.uk).

# **Can I operate CCTV on my private property?**

**Yes you can.**

However if you are capturing images outside of your property boundary or if you are operating a business from your property this may make you a data controller for the purposes of the Data Protection Act 2018 (DPA), and to ensure compliance with the DPA you would need to:

- Consider what area needs to be covered and what images will be captured,
- Safeguard any recorded images to enable usage by the police to investigate crimes affecting you,
- Install signage that indicates CCTV is operational in the area,
- Ensure the footage recorded is stored securely and only individuals access the data who need to

Be able to respond appropriately to a request for the footage from individuals who appear in it (this is known as a subject access request and further information on this can be found on our website), and

If audio facilities are active on CCTV systems, the ICO recommends the surveillance systems should not normally be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified.

Unless you can clearly justify the use of audio with robust supporting evidence this type of recording should not be used.

We would also remind you that if there is a requirement for you to comply with the DPA, this would include the need to respond to any subject access request you may receive.

Under Article 15 of the UK General Data Protection Regulations (UK GDPR) an individual is entitled to request a copy of the personal data that a data controller is holding about them. This is known as a subject access request. A data controller should respond promptly and in any event within a month of receiving it. You should supply the requester with a copy of the personal data requested if you are holding it, unless an exemption applies.

Our guidance about Article 15 of the UK GDPR can be found at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/>

# The Children’s Code - Procedures for Public Advice and Data Protection Complaints Services

## Contents

<b>1. Procedure for live services and social media for contact from children or about the Children’s Code</b> .....	3
1.1 Establishing if the contact is from a child.....	3
1.2 Children’s Code advice and complaints .....	3
1.3 Data protection advice and complaints .....	3
1.4 Wrong number / Incorrectly signposted / Not for the ICO.....	4
1.5 Safeguarding concerns.....	4
(a) Line to take for a child.....	5
(b) Line to take for a concern raised on behalf of a child.....	5
<b>2. Procedure for advice cases from children or in relation to the Children’s Code</b> .....	6
2.1 Channels for enquiries from children.....	6
2.2 Corresponding with children .....	6
2.3 Responding to enquiries from children .....	6
2.4 Responding to enquires about the Children’s Code.....	6
2.5 Safeguarding concerns and misdirected contacts.....	6
<b>3. Procedure for complaints from or about children</b> .....	8
3.1 Channels for complaints directly from children.....	8
3.2 Sifting complaints from children.....	8
3.3 Case set up and authority to act on behalf of a child .....	8
3.4 Process for complaints sent to the Children’s Complaints inbox.....	9
(a) Complaints solely about the Children’s Code.....	9
(b) Complaints about the Children’s code that also include general data protection concerns.....	10
(c) Complaints directly from children.....	10
3.5 Corresponding with children .....	11
3.6 Safeguarding concerns.....	11
<b>4. Safeguarding and useful contacts for signposting</b> .....	12
4.1 Childline .....	12
4.2 NSPCC.....	12
4.3 Reporting to police.....	12

4.4 Child Exploitation and Online Protection Command (CEOP).....	12
4.5 Thinkuknow .....	13
4.6 Report Harmful Content.....	13
4.7 UK Safer Internet Centre .....	13
4.8 Internet Watch Foundation (IWF).....	13
4.9 Action Counters Terrorism.....	13

## **1. Procedure for live services and social media for contact from children or about the Children's Code**

### 1.1 Establishing if the contact is from a child

It might not always be clear if you are speaking to a child when on live services. If you think it may be a child, you can ask if they are under 18 if this will help answer the query or provide an appropriate response.

Please ensure that a wrap form is completed for every contact from a child or about the Children's Code.

### 1.2 Children's Code advice and complaints

If you receive a call about the Children's Code, you can select this on the call wrap. A link is provided to our website which details each of the [Age Appropriate Design Code \(AADC\) standards](#). You can select all standards that apply on the wrap form.

The information collected will be shared with [Operation Valency](#).

### 1.3 Data protection advice and complaints

If the child is raising a general data protection concern, the normal process for handling advice and complaints will apply.

When talking to children try to avoid using 'jargon'. Use plain, simple and clear language to help the child understand their rights and what they can do if they are unhappy about how their personal data has been used.

You can direct children to our website using the relevant links for advice and template letters, explaining how they can complain to the organisation and to the ICO if they remain unhappy.

We should also provide advice on how to find contact details for the organisation they want to contact or complain to. For example, directing children to the privacy policy. If they have confirmed the organisation, we can direct them to their privacy policy or provide a link. If there is an email address publicly available for the data protection team or Data Protection Officer (DPO) it may be helpful to highlight this.

However, we should always be clear that they need to be sure it is the correct company themselves before contacting them.

We can direct children to use the ICO complaint form, providing a direct link, however it may not always be possible for them to use it. Therefore, children may prefer to raise a complaint with us via live services.



If a child wants to make a complaint via live services or social media, the complaint form should be filled in including contact details for the child. As we will not be able to respond to complaints via live chat or social media, it is important to ask for a postal address or an email address.

It should be made clear to children that we will require evidence to show that they have raised their concerns with the organisation before we can look into the complaint. We should provide our email address, postal address for them to provide evidence.

If the child has contacted us via direct message (DM) on social media, they can provide evidence through this channel that can be copied on to the case.

The case should be created on ICE and the case reference sent to

#### 1.4 Wrong number / Incorrectly signposted / Not for the ICO

There is a possibility that a child, or someone acting on behalf of a child, may contact us in error, trying to get hold of another organisation, or believe that the issue is for the ICO but it falls outside our remit.

When possible, try to signpost the child to the appropriate organisation, providing contact details if they are available. A list of organisations that may be useful to signpost misdirected calls from, or about, children is available on [SharePoint](#). Details are also included in [section 4](#).

Details about the nature of the call, including the organisation if known, should be included on the wrap form.

#### 1.5 Safeguarding concerns

It is unlikely, but there is a possibility that a child may call and make a disclosure about their wellbeing or safety. In this case you should direct them, or the person calling on their behalf, to Childline or the NSPCC respectively.

More information about the different organisations we can signpost individuals to in relation to safeguarding concerns can be found in [section 4](#).

As soon as you become aware that the issue is not something the ICO can help with, you can interrupt the caller to explain this. This will prevent the individual having to explain the situation in full which may be difficult or distressing for them, especially as they will have to explain again to another organisation.

You can acknowledge the concerns raised, and reassure them that the NSPCC or Childline will listen to their concerns and take them seriously. However, it is important not to ask questions about any safeguarding issues or say that you can help.

The lines to take are available on the wrap form by selecting 'Not ICO – safeguarding concern'.

#### (a) Line to take for a child

“Thank you for your call/contacting us, you’ve been really brave to try to talk to us and you have done the right thing in telling an adult.

I’m going to have to stop you there as I’m not the right person to help you with this, and after being so brave, I don’t want you having to repeat yourself as I understand it is difficult to talk about.

You can speak to Childline who can support you with this. You can call them on 0800 1111, use online chat or email them from their website: <https://www.childline.org.uk/get-support/>”

#### (b) Line to take for a concern raised on behalf of a child

“Thank you for your call/message today. I’m going to have to stop you there as I’m not the right person to help you with this, and I don’t want you having to repeat yourself as I understand it is difficult to talk about.

The best place to contact in this situation is the NSPCC. You can call them on 0808 800 5000 or visit their website for other contact methods: [www.nspcc.org.uk](http://www.nspcc.org.uk)”

## 2. Procedure for advice cases from children or in relation to the Children's Code

### 2.1 Channels for enquiries from children

Children may prefer to make enquiries via social media or live chat, however may also receive enquiries by email or via the helpline from children.

We may receive enquires about the Children's Code from individuals or from Civil Society Groups.

### 2.2 Corresponding with children

All correspondence should be written following the ICO style guide.

Use plain vocabulary and consider any particular needs of the individual complaining.

Particular care should be taken to avoid jargon. If specific terms need to be used they should be explained clearly.

Where appropriate, icons can be used to help keep the information clear and understandable. Icons should be used consistently across all ICO services including the website, social media and in correspondence.

### 2.3 Responding to enquiries from children

Enquiries directly from children should be handled in line with the normal enquiries procedure. Provide simple, clear information and signpost to our website to help children exercise their rights and raise concerns with organisations.

### 2.4 Responding to enquires about the Children's Code

Enquiries about the Children's Code should be handled as per the normal process, directing to our website as appropriate.

If you receive any correspondence that is potentially linked to the code, or from a civil society group, please send a copy of it to the Operation Valency Inbox at:

### 2.5 Safeguarding concerns and misdirected contacts

If a child makes a disclosure about their wellbeing or safety this should be sent to  for consideration.

The disclosure will be considered and discussed with a Group Manager. If required, we will inform the child that we will need to share their

information with an organisation that can help. This will then be reported to the most appropriate body, detailed in [section 4](#).

If the issue is not something we can help with, we should signpost children and adults to an appropriate organisation wherever possible. A list of organisations is available on [SharePoint](#). Details are also included in [section 4](#).

## 3. Procedure for complaints from or about children

### 3.1 Channels for complaints directly from children

We may receive complaints from children via live services, the complaint form, email or post.

### 3.2 Sifting complaints from children

Complaints from children, or in relation to the Children's Code (the Code), formally known as the Age Appropriate Design Code (AADC), will be identified at the point of sifting complaints.

As a new code of practice, it is important to gather information quickly to help support organisations and deepen our understanding of the type of concerns that may arise following its introduction.

Complaints from children, or about the code, will be handled without delay and will not wait for allocation with other complaints.

If a complaint from a child waits in a queue for a few months, this could mean that their complaint will not be resolved for a long time. This may have a big impact on a child's life while waiting for the outcome. It is in the best interests of the child to look at these without delay.

If a complaint contains a safeguarding disclosure, this needs to be addressed as soon as possible as we may need to report this to an appropriate body.

Once the case has been created in line with the normal case creation procedure, the case reference should be sent to

\_\_\_\_\_

Information to assist with identifying these complaints is available on [SharePoint](#).

This procedure does not apply to complaints raised on behalf of children in relation to general data protection concerns. These will be handled as per the normal complaint procedure.

### 3.3 Case set up and authority to act on behalf of a child

If the complaint is about a child's personal data ensure that this is recorded correctly on the case information page. The age category should also be filled in if known.

We also need to consider whether we need authority from the child before proceeding with the complaint.

The general rule in the UK is that organisations should consider whether the individual child has the competence to understand and consent for themselves.

In Scotland, children aged 12 or over are presumed to be of sufficient age and maturity to exercise their data protection rights (unless the contrary is shown).

This is separate to the provision in Article 8 on children's consent for Information Society Services (ISS). Where an organisation wants to rely on consent rather than another lawful basis for processing personal information, it must get parental consent for children under 13.

Therefore, for complaints made on behalf of children aged 12 or over, we should consider asking the person submitting the complaint to provide proof that the child has specifically authorised them to complain to the ICO (such as a letter giving them authority to do so), unless advised otherwise. An example is given below.

However, it is important to always consider each case individually based on the specific circumstances and nature of the complaint.

Example:

If you feel that XX is able to understand and consent for you to complain to the ICO on his/her behalf, we will require proof that he/she has specifically authorised you to do so.

Authority can be provided by phone, an email from xxx using his/her own email address including the case reference in the subject line, or a signed paper statement.

However, if you think that XX will not be able to understand and consent, please confirm this in your response.

### 3.4 Process for complaints sent to the Children's Complaints inbox

Complaints sent to the Children's Code Complaints inbox will be checked within two weeks and allocated to a specified case officer (SPOC) within Public Advice and Data Protection Complaints Services.

#### (a) Complaints solely about the Children's Code

Complaints solely relating to organisations conforming with the Code will be referred to Operation Valency for consideration after the case has been created.

Once the case is allocated, if it has already been referred to Operation Valency, we should contact them to see if the organisation has been included in their sweep work.

If it has then no further action is required, and correspondence can be sent to the complainant explaining that their concerns have been passed to the relevant department. If there are no outstanding issues, we will inform the complainant that there is no further action at this stage. The case should be closed and a note added to explain the reasons for closure.

If it was not included in the sweep work, we will proceed with the case in line with our normal casework procedures. Additional policy information can be sought from by sending an email to

\_\_\_\_\_ Policy or Operation Valency.

#### (b) Complaints about the Children's code that also include general data protection concerns.

If we receive a complaint from an adult raising concerns about the code, alongside general data protection issues (eg non-response to a SAR), a copy will be sent to Operation Valency. This will be noted on the case and be returned to the queue to await allocation. It should then be handled as per the normal procedure.

If you receive any correspondence that is potentially linked to the code, please send a copy of it to the Operation Valency Inbox at:

\_\_\_\_\_

#### (c) Complaints directly from children

Complaints from children should be investigated in line with our normal complaint handling procedure by a specified case officer (SPOC).

Adjustments should be made, where possible, to ensure children are not waiting lengthy periods for responding.

Correspondence should be sent to the complainant within two weeks of the complaint being allocated.

If there is not enough information to proceed, information and advice should be provided to help them exercise their rights and raise concerns with organisations.

It should be made clear to children how long we expect it will take for us to reach a decision and regular updates should be provided in case of any unexpected delays.

Long investigations should be avoided if possible. If further evidence is required from the data controller, this should be requested as soon as possible and in any case within two weeks.

### 3.5 Corresponding with children

All correspondence should be written following the ICO style guide.

Use plain vocabulary and consider any particular needs of the individual complaining, ensuring that we are providing age appropriate information.

Particular care should be taken to avoid ICO jargon. If specific terms need to be used they should be explained clearly.

Where appropriate, icons can be used to help keep the information clear and easy to understand. Icons should be used consistently across all ICO services including the website, social media and direct correspondence.

### 3.6 Safeguarding concerns

If a child makes a disclosure about their wellbeing or safety this should be sent to \_\_\_\_\_ for consideration.

The disclosure will be considered and discussed with a Group Manager. If required, we will inform the child that we will need to share their information with an organisation that can help. This will then be reported to the most appropriate body, detailed in [section 4](#).



## 4. Safeguarding and useful contacts for signposting

If a child makes a disclosure about their wellbeing or safety this should be sent to \_\_\_\_\_ for consideration.

The disclosure will be considered and discussed with a Group Manager. If required, we will inform the child that we will need to share their information with an organisation that can help. This will then be reported to the most appropriate body, detailed in [section 4](#).

### 4.1 Childline

Childline is a free and confidential service available to help anyone under 19 in the UK with any issue they're going through. Children and young people can talk to Childline about anything and is available at any time, day or night. They can contact Childline by calling 0800 1111, by email or through 1-2-1 counsellor chat: <https://www.childline.org.uk/>

### 4.2 NSPCC

The NSPCC is the UK's leading children's charity. If someone is worried about a child, even if they are unsure, they can speak to the NSPCC about their concerns: <https://www.nspcc.org.uk/keeping-children-safe/reporting-abuse/>

### 4.3 Reporting to police

If a child is in immediate danger please call the police on 999 straight away.

### 4.4 Child Exploitation and Online Protection Command (CEOP)

CEOP keeps children safe from sexual abuse and grooming online. If something has happened to a child online which makes them feel unsafe, scared or worried, they can make a report directly to CEOP. All reports are taken seriously and they will do everything they can to keep the child safe: <https://www.ceop.police.uk/Safety-Centre>

Some of the things children and young people have reported to CEOP include:

- Someone online has asked a child or young person to send them nude images or videos
- A child or young person has shared a nude image or video online and they are threatening them
- Someone the child knows offline, such as someone they were/are in a relationship with or a peer, has shared a nude image or video of them via phones or online

- Someone a child doesn't know has asked them to live-stream and do things they don't want to do
- Someone online is pressuring a child or young person to meet them face-to-face
- Someone online is talking to a child or young person about sex and has made them feel uncomfortable
- Someone a child or young person has met in an online game keeps trying to talk to them privately

CEOP are unable to respond to reports about bullying, fake accounts or account hacking. Concerns of this nature can be reported via Report Harmful Content, detailed below.

#### 4.5 Thinkuknow

If parents or children require more information on staying safe online we can signpost them to the Thinkuknow website. It has information and advice for parents, professionals, and children and young people to help them stay safer online: <http://www.thinkuknow.co.uk/>

#### 4.6 Report Harmful Content

"Harmful content is anything online which causes a person distress or harm"

Provided by [UK Safer Internet Centre](#) and operated by [SWGfL](#), it provides up to date information on community standards and direct links to the correct reporting facilities across multiple platforms. Also provides further support to users over the age of 13 who have already submitted a report to industry and would like outcomes reviewed:

<https://reportharmfulcontent.com/>

#### 4.7 UK Safer Internet Centre

Provides online safety tips, advice and resources to help children and young people stay safe online: <https://www.saferinternet.org.uk/>

#### 4.8 Internet Watch Foundation (IWF)

For reporting child sexual abuse pictures or videos on the internet or non-photographic child sexual abuse images: <https://www.iwf.org.uk/>

#### 4.9 Action Counters Terrorism

For reporting terrorist or extremist content online: <https://act.campaign.gov.uk/>

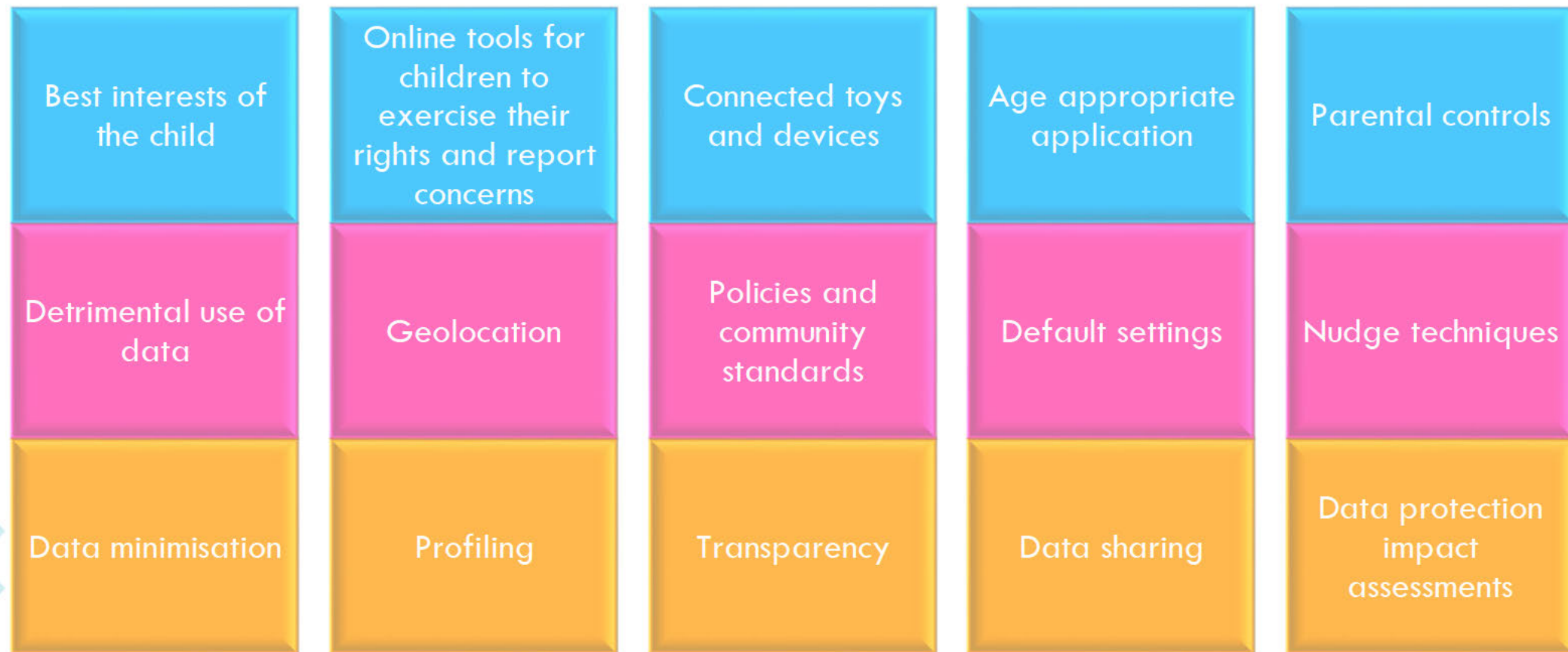


## Public Advice and Data Protection Complaints and the Children's Code



# The Children's Code

- The Children's code (or the Age appropriate design code) contains 15 standards that online services need to follow. This ensures they are complying with their obligations under data protection law to protect children's data online





# Introduction

- The code applies to information society services (ISS) including apps, online games, connected toys, social media, websites offering goods and services and search engines
- If children are likely to access the service, even if they are not the target audience or user, then the organisation needs to consider the Children's code
- The code applies to UK-based companies and non-UK companies who process the personal data of UK children
- Organisations may need to think about:
  - Mapping the personal data collected from UK children
  - Checking the age of those accessing the service
  - Switching off geolocation services
  - Not using nudge techniques to encourage children provide more personal data
  - Providing a high level of privacy by default



# Operation Valency

- They have contacted around 50 organisations with questions around how they are conforming with the code. They refer to this as a 'sweep'
- They are focussing on three main areas:
  - Gaming
  - Social media
  - Streaming
- They can consider adding more organisations to their 'sweep' work by emailing concerns to \_\_\_\_\_
- They gather information on the types of concerns being raised with the ICO from advice cases and complaints
- Information from the call wraps on the helpline is collated and provided to them as required
- Their main focus is 'data protection by design'



# Live services and advice cases

- Use the links available on the call wrap and log accordingly
- Advice cases - send an email to  for reference and for any advice
- Send details about the issue raised to  for their information
- Things to consider:
  - Does the code apply? Is it an online service/a child's data/in the UK?
  - Is it an online harms concern?
- Direct to the Children's code guidance on our website
- Advise to raise concerns with the organisation first, then with us



# Promoting the Code

- The ICO commissioned two external organisations to complete research with parents and children to help understand the issues they may have experienced
- Overall, there was very little awareness about the code, or what the ICO could do to help if something went wrong
- All children had experienced their data being misused, including unwanted friend requests, receiving adverts based on location and getting hacked
- One parent said “You aren’t going to complain that your rights aren’t being upheld if you don’t know they exist”
- If people don’t know about the code, or what the ICO do, then they won’t bring complaints about children’s data to us
- We should therefore promote the code, directing people to our guidance if it appears that it could be relevant





# Case creation

- Could the complaint be from a child (under 18)?
  - Send the reference to
  - Complaints directly from children will be responded to within two weeks
  - Complaints made on behalf of children do not need to be referred
- Is the complaint about the Children's Code, AADC?
  - Send the reference to
  - Operation Valency will be made aware of the complaint and this will be noted on the complaint
  - The case will await allocation as normal, once allocated the case officer should contact Op Valency to see if it was picked up in the sweep



# Complaints

- Individual concerns will be handled by PADPCS in most circumstances
- We will refer to complaints to Operation Valency for awareness and consideration
- If it has already been referred, contact Op Valency to see if it has been included in the sweep
  - If it has been included, we can confirm to the DS that their concern has been passed to the relevant department and they are making enquiries
  - If they have not included it, we can proceed with the case as a normal complaint



# Outcomes for complaints

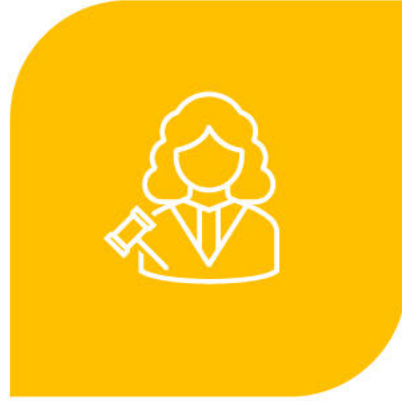
- It is a statutory code of practice, not the law, but the ICO (and courts) must take it into account when assessing complaints about the processing of children's data by ISS
- GDPR Recital 38 says: 'Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.....'
- Organisations should **conform** with the code and **comply** with UK GDPR
- If they cannot demonstrate how they meet the expectations of the standards, or demonstrate how they protect children's data otherwise, then it is unlikely that they are complying with the UK GDPR, particularly Article 5(1) that processing must be lawful, fair and transparent



# Example outcome



An organisation has not provided privacy information to children, they only have a detailed privacy policy containing many technical and legal terms.



In this case, they will not have not complied because the processing is not fair and transparent.



This is because they are not conforming with standard 4 (transparency) of the age appropriate design code as they have not provided information in a child friendly way. Further, it is not sufficient to rely on children or their parents seeking out privacy information.



# Do they process children's data?

- The code covers services that are likely to be accessed by UK children
  - This depends upon:
    - Nature, content and presentation of service
    - Any measures in place to prevent children gaining access
  - Legal test:
    - More probable than not
  - Accountability:
    - Document decision & reasoning
- We can ask organisations if they have considered how likely children are to access their service and what measures they have to protect children's data, eg by preventing access or having high privacy settings by default.



## Territorial scope

- In scope:
  - UK based
  - International, with UK office, and product offered to UK users
  - International, with no UK office, no EEA office, and product offered to uk users
- Out of scope (for now):
  - International, with no UK office, but office in EEA
- If providing advice (live services or enquiries), and it isn't clear if the organisation falls within scope but is based in America, you can provide the link to our statement on California's age appropriate design code: [ICO statement on California's plans to introduce new bill to protect children's data online | ICO](#)



# Recent examples

**Zwift** – concerns about the amount of data they require from children. This included age, height and weight in order to play a cycling game. This information is then used to celebrate weight loss.

**WikiHow** – concerns about privacy information provided to children that may access the service and how they would use their data.

**SnapChat** – Child concerned that her account was hacked and personal images were shared online. Doesn't really fall under the code, although security would be a concern, as she wanted the images removed from the internet. Referred to organisations that can help.

**Instagram** – not preventing children from accessing harmful content. This will fall under the upcoming Online Safety Bill. We are awaiting a joint statement from Ofcom and the ICO.



## **Acknowledgement (ICE enquiry)**

Thank you for your email of [Insert date] regarding your concerns about [brief description of concerns].

The further documentation you have sent in to case reference **IC-XXXXX-XXXX** is now being considered as a concern under the above reference: **IC-XXXXX-XXXX**. This will be assigned to one of our casework teams before being allocated to a case officer who will respond in due course.

**Please note;** should you wish to contact us about this matter please quote the above case reference number **IC-XXXXX-XXXX**. Failure to do so may delay the processing of your request.

If you require any further advice or assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Name  
Job Title  
Information Commissioner's Office

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice).

## **Acknowledgement (CMEH enquiry)**

Thank you for your email of [Insert date] regarding your concerns about [brief description of concerns].

The further documentation you have sent in to case reference **ENQXXXXXX** is now being considered as a concern under the above reference: **IC-XXXXX-XXXX**. This will be assigned to one of our casework teams before being allocated to a case officer who will respond in due course.

**Please note;** should you wish to contact us about this matter please quote the above case reference number **IC-XXXXX-XXXX**. Failure to do so may delay the processing of your request.

If you require any further advice or assistance please contact our



Helpline on 0303 123 1113.

Yours sincerely

Name

Job Title

Information Commissioner's Office

For information about what we do with personal data see our  
privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice).

## **Domestic CCTV fact sheet**

Where an individual is using CCTV cameras, fixed to their property, that capture images **beyond the boundaries** of their property, they are required to comply with data protection legislation.

When we receive a complaint from an individual we will contact the neighbour, informing them of their obligations should the camera capture images outside of their property boundary. We will go no further than this.

We cannot, under any circumstances, ask an individual to remove or reposition cameras.

If an individual feels harassed/intimidated they should speak to the police.

### **FAQ's:**

Are smart doorbells covered? – Yes, if it captures images outside of the property boundary. Note: a communal space such as a corridor/shared garden would be considered outside of the property boundary.

Do camera operators need to register? – No, unless it's a business.

Will the ICO ask to see what the cameras are capturing? – No.

Can I provide images of my neighbours cameras? - You can, but they are not required and will not alter the handling of the complaint.

What about shared access areas? – You would be required to comply if you're capturing images where there is shared access. This includes where someone has a 'right of way' (such as a driveway).

[Domestic CCTV systems - guidance for people using CCTV](#)

[Domestic CCTV systems – guidance for people being filmed](#)

Should you require further information ask Karen Shann or Ian Johnson.

## The Information Commissioner's powers

Data protection incidents which occurred prior to 25 May 2018 fall under the Data Protection Act 1998 (the DPA 1998) which was in place until that date. Incidents which occurred on or after 25 May fall under the General Data Protection Regulation (the GDPR) and/or the Data Protection Act 2018 (the DPA 2018), which we refer to as the 'data protection legislation', depending on the nature of the processing involved.

There are a number of powers available to the Information Commissioner's Office (ICO) in respect of breaches of the data protection legislation.

Our powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

The main options are to:

- provide practical **advice** to organisations on how they should handle data protection matters;
- conduct **consensual assessments** (audits) to assess whether an organisation's processing of personal data follows good practice;
- issue **information notices** requiring individuals, controllers or processors to provide information as part of an investigation into compliance with the data protection legislation. If the recipient of an information notice does not provide a full and timely response, the ICO may apply for a court order requiring compliance with the information notice;
- issue **assessment notices** to allow us to investigate whether a controller or processor is compliant with data protection legislation. The notice may, for example, require the controller or processor to give us access to premises and specified documentation and equipment.
- issue **warnings** where proposed action threatens non-compliance with data protection legislation;
- issue **reprimands** for infringements of relevant data protection legislation;
- issue **enforcement notices** where there has been an infringement, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the data protection legislation;

- issue **penalty notices** requiring organisations to pay administrative fines of up to 20 million Euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover, depending on the nature of the infringement; and
- **prosecute** those who commit criminal offences under the data protection legislation. In Scotland, where the ICO is satisfied that there are grounds for a prosecution, it will make a report to the Procurator Fiscal to make a determination whether or not to prosecute.

Information about our chosen approach to regulatory action can be found in ICO's draft Regulatory Action Policy which gives direction and focus to the organisations it regulates.

Information about action we have taken can also be found on our website:

<https://ico.org.uk/action-weve-taken/>

## Template letter – how to complain

Updated Aug 2020

### How to complain standard letter

This letter can be used if we need more information from an individual to enable us to look into their data protection complaint. It can be amended dependant on the circumstances of the case.

If it is clear that we cannot consider part of the individual's complaint they should be informed of this and redirected where appropriate.

.....

### Further information required

Dear xxx

Thank you for your email/letter of [date] regarding a complaint about a data protection matter.

Before we can consider your complaint we need additional information from you. Please reply to this email, quoting the above reference number with **all** of the following:

- The name and address of the organisation your complaint is about.
- Copies of any letters or emails you sent to the organisation complaining about this matter.
- Copies of any letters or emails they sent back, showing their complaints process has ended.

If you have not yet complained to the organisation we would strongly recommend that you do so to give them the chance to put things right before raising this matter with us. We have information on [how to make a data protection complaint to an organisation](#) that may help you with this.

Without this information we may be unable to consider this matter further.

If you require any further advice or assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

XXXXXXXXXXXX

Please consider the environment before printing this email

For information about what we do with personal data see our [privacy notice](#)

## **How to improve Listening and interpreting complaints checklist**

1. To improve listening at the receiving stage,
  - prepare yourself to listen,
  - discern between intentional messages,
  - concentrate on stimuli most relevant to your listening purpose(s) or goal(s),
  - be mindful of the selection and attention process as much as possible,
  - avoid interrupting someone while they are speaking in order to maintain your ability to receive stimuli and listen.
  
2. To improve listening at the interpreting stage,
  - identify main points and supporting points;
  - use contextual clues from the person or environment to discern additional meaning;
  - be aware of how a relational, cultural, or situational context can influence;
  - note differences in tone of voice and other paralinguistic cues that influence meaning.
  
3. To improve listening at the recalling stage,
  - repeat, rephrase, and reorganize information to fit your cognitive preferences; and
  - use a gimmick to help with recall.
  
4. To improve listening at the evaluating stage,
  - separate facts, inferences, and judgments;
  - be familiar with and able to identify persuasive strategies and fallacies of reasoning;
  - assess the credibility of the speaker and the message; and
  - be aware of your own biases and how your perceptual filters can create barriers to effective listening.
  
5. To improve listening at the responding stage,
  - ask appropriate clarifying and follow-up questions and paraphrase information to check understanding,
  - give feedback that is relevant to the speaker's purpose/motivation for speaking,
  - adapt your response to the speaker and the context, and
  - do not let the preparation and rehearsal of your response diminish earlier stages of listening.
  
6. To improve conveying a difficult message
  - Plan what you are going to say
  - Consider the possible impact of your message
  - Anticipate the likely reaction (emotions)
  - Be clear/concise in the delivery of your message
  - Give reasons for your action/decision
  - Allow a response and demonstrate that you understand the reaction (but don't necessarily agree with it)

7. Following the call,
  - What aspects of the contact did you handle particularly well and why?
  - What areas could you improve on?
  - What would you do differently?



## **ICO Statement**

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Any correspondence, letters, emails and notes of phone calls, may be considered for disclosure. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do. It should be noted, the ICO will not release any information unless we have the lawful authority to do so.

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice)

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link: [Complaints and concerns data sets | ICO](#).

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at [accessicoinformation@ico.org.uk](mailto:accessicoinformation@ico.org.uk). We will only agree to this in limited circumstances where we are satisfied that the interests of the parties involved would override the ICO's obligations to publish this information.

**ico.**  
Information Commissioner's Office  
children's  
code



## GETTING READY FOR THE CHILDREN'S CODE

HINTS AND TIPS FOR IDENTIFYING COMPLAINTS IN  
RELATION TO THE AGE APPROPRIATE DESIGN CODE  
AND COMPLAINTS DIRECTLY FROM CHILDREN.



**WHY DO WE NEED TO SIFT OUT  
COMPLAINTS ABOUT THE CHILDREN'S  
CODE AND THOSE DIRECTLY FROM  
CHILDREN?**

## COMPLAINTS ABOUT THE CHILDREN'S CODE

Complaints about the Children's Code will be looked at by a dedicated team.

As a new code of practice, it is important to gather information quickly to help support organisations and deepen our understanding of the type of concerns that may arise following its introduction.

## COMPLAINTS FROM CHILDREN

If a complaint from a child waits in a queue for a few months, this may mean that their complaint will not be resolved for a long time. It could have a big impact on a child's life while waiting for the outcome.

It is in the best interests of the child to look at these without delay.

It is very unlikely, but if a complaint contains a safeguarding disclosure, we may need to report this to an appropriate body.

If a child is at immediate risk we can contact the police, waiting in the queue could cause serious harm if the child thinks they have told someone who can help.

## COMPLAINTS RAISED ON BEHALF OF CHILDREN

We don't need to sift out complaints raised on behalf of children, unless they relate to the Children's Code.



These can be handled as normal and await a case officer in the relevant queue.

## HOW TO RECOGNISE COMPLAINTS FOR SIFTING

We might not always be able to recognise complaints from children, and not all complaints that relate to the code will be obvious.

By looking at the following areas can help with identifying these complaints:



The complaint form



Complaint details



Evidence provided



Key words and phrases

## THE COMPLAINT FORM

I/person making this complaint was 17 or under

Tick if the person making the complaint was aged 17 or under at the time they made their request or complaint to the organisation. We use this to understand if the complaint relates to the rights of children.

This is a good starting point for picking out complaints to look at in slightly more detail, however not all complaints about children's data need to be sifted out.

Not all complaints from/about children will have ticked this box, also some adults tick it incorrectly!

Sometimes it is obvious that it isn't about a child's data. Eg "It has been 6 years since my bankruptcy, but it is still showing on my credit report."



## ORGANISATIONS OF INTEREST

Some organisations have already been highlighted as falling under the Code in the media including TikTok, Instagram, Facebook, Google and YouTube (Kids).

Complaints from civil society groups: 5Rights Foundation, Privacy Matters, Open Rights Group

Sectors that are more likely to include complaints from children: DP1 - Schools, Education Technology, DP3 – Social Services, DP5 – Search Engines, Social Media, DP6 – Foster Care, Health

## COMPLAINT DETAILS



Check the details of the complaint on the complaint form/email for obvious references to the code



Look out for any reference to the age of the complainant, direct or indirect. Eg "my teacher/mum/dad"



Look out for key phrases from the code (see list provided)



Current themes emerging:  
Private accounts by default including who can see social media posts, geolocation, targeted advertising to kids, etc.

## EVIDENCE PROVIDED

Scan the evidence provided as a final check for complaints from children or about the code

Check for indications of age, could it be from a child?

Check for references to the Children's Code, Age Appropriate Design Code (AADC)

Check for key words and phrases

## KEY WORDS AND PHRASES FROM THE CODE

Key words and phrases can be used alongside other indicators, particularly if the complaint is unclear. The ones at the top are more likely to indicate complaints about the Children's Code.

Best interests of the child	Online tools for children to exercise their rights and report concerns	Connected toys and devices	Age appropriate application	Parental controls
Detrimental use of data	Geolocation	Policies and community standards	Default settings	Nudge techniques
Data minimisation	Profiling	Transparency	Data sharing	Data protection impact assessments

## UNCLEAR FOLLOWING INITIAL CHECKS?

Ask a colleague, the more cases we see the easier it will be to spot complaints from children or about the code

Complaints that raise any concerns about risk to a child, or if someone is reporting a safeguarding concern, can always be sent over for checking

If you have done all the checks suggested, and you are still unsure, then send the reference number over for checking



## WHAT TO DO NEXT

Send the case reference numbers for complaints from children, or relating to the code, to

If there is doubt, please give a brief description in the email.

As we gain more understanding about the nature and types of complaints we receive, this information will be updated.

Dear

Thank you for submitting a complaint about the processing of your personal information. We understand how important this is to you.

We have considered the issues you have raised but have not been able to decide whether there has been an infringement of data protection law. This is because we need to see the evidence to support your complaint.

There are two options for what you need to do next, depending on whether you have already complained to the organisation:

- **If you have not yet complained to the organisation**

If you have not yet complained to the organisation, we strongly recommend that you do so to give them the chance to put things right. We have information on [how to make a data protection complaint to an organisation](#) that may help you to do this.

We always want to allow organisations the opportunity to resolve matters with you and we expect that most cases will be resolved without our intervention. Organisations should work with you to explain how they have handled your personal data, and help you to exercise your rights properly.

- **If you have already complained to the organisation**

If you have received a final response from the organisation, and they have stated that they will not look at matters further, then please come back to us.

We need you to send us copies of letters or emails you've sent to the organisation explaining what your information rights complaint is. It is important that you include any final response that the organisation has sent to you.

Please quote the reference number at the top of this letter on any future correspondence about this matter.

We fully expect that most cases can be resolved without our intervention. We will now close this complaint. However, it will be revisited if you aren't able to get matters resolved and you send the supporting evidence we need.

If you require any further advice or assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Xxx



## Signposting for misdirected queries on social media

### Concerns raised about keeping children safe online and harmful content

Organisation	Website
Thinkuknow	<a href="https://www.thinkuknow.co.uk/">https://www.thinkuknow.co.uk/</a>
Report Harmful Content	<a href="https://reportharmfulcontent.com/">https://reportharmfulcontent.com/</a>
UK Safer Internet Centre	<a href="https://www.saferinternet.org.uk/">https://www.saferinternet.org.uk/</a>

### Concerns raised about a child's safety

Organisation	Website
Childline	<a href="https://www.childline.org.uk/">https://www.childline.org.uk/</a>
NSPCC	<a href="https://www.nspcc.org.uk/">https://www.nspcc.org.uk/</a>
CEOP	<a href="https://www.ceop.police.uk/Safety-Centre">https://www.ceop.police.uk/Safety-Centre</a>
Internet Watch Foundation (IWF)	<a href="https://www.iwf.org.uk/">https://www.iwf.org.uk/</a>
Action Counters Terrorism	<a href="https://act.campaign.gov.uk/">https://act.campaign.gov.uk/</a>

ent

**Details**

Provides information and advice for parents, professionals, and children and young people to help them stay safer online

"Harmful content is anything online which causes a person distress or harm" provides up to date information on community standards and direct links to the correct reporting facilities across multiple platforms. Also provides further support to users over the age

Online safety tips, advice and resources to help children and young people stay safe online

**Details**

Available to help anyone under 19 in the UK with any issue they're going through

For anyone worried about a child's safety

Keeps children safe from sexual abuse and grooming online. If something has happened to a child online which makes them feel unsafe, scared or worried, they can make a report to CEOP. They can't respond to reports about bullying, fake accounts or account

For reporting child sexual abuse pictures or videos on the internet or non-photographic child sexual abuse images

For reporting terrorist or extremist content online

## General Misdirected template

Misdirected template letter.

Thank you for your letter of-----about -----

Unfortunately this is not a matter that we can help you with. [Please find enclosed your original documents. - only if required]

The Information Commissioner's Office enforces and oversees the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000.

We only hold information in relation to concerns made to us about organisations compliance with the legislation and the guidance that we produce about the legislation. We do not operate as a general source of information or as a store for information held by other public authorities. [Only use italic paragraph for misdirected information requests or misdirected subject access requests.]

In this case it appears that you may need to contact -----

I hope this information is helpful to you. If you need advice on a new issue you can contact us via our Helpline on 0303 123 1113 or through our live chat service. In addition, more information about the Information Commissioner's Office and the legislation we oversee is available on our website at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely

[Insert staff name]  
Case Officer  
Information Commissioner's Office

For information about what we do with personal data see our privacy notice on our website:

<https://ico.org.uk/global/privacy-notice/>

## **Misdirected Freedom of Information Scotland (FOISA) requests**

Thank you for your email of [date]. This was sent to the Information Commissioner's Office.

The Information Commissioner's Office enforces and oversees the General Data Protection Regulations, the Data Protection Act 2018 and the Freedom of Information Act 2000. Public authorities in Scotland which relate to devolved matters are subject to the Freedom of Information (Scotland) Act 2002 which is regulated by the Scottish Information Commissioner.

I hope this information is helpful to you. If you need advice on a new issue you can contact us via our Helpline on 0303 123 1113 or through our live chat service. In addition, more information about the Information Commissioner's Office and the legislation we oversee is available on our website at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely

Name  
Case Officer  
Information Commissioner's Office

For information about what we do with personal data see our [privacy notice](#)

### **FOI**

The Freedom of Information Act 2000 (FOIA) is to do with transparency of information held by public authorities. It enables people to access recorded information (other than personal data) held by public authorities. For example you could use the FOIA to request information from your local council about their budgets or policies.

However I must point out, we do not hold public information at our office unless we have had previous contact. If you are looking for information that may fall under the FOIA then you need to send your request to the appropriate organisation/authority that holds the information.

I have provided a link to our website about how to access information using the FOIA <https://ico.org.uk/your-data-matters/official-information/>.

## **Credit**

If you believe that information held on your file is not correct, you should, in the first instance, write to the credit reference agency or the lender and explain to them why you believe the information is wrong. Keep copies of any letters you send together with any replies you receive.

If you write to the credit reference agency, it will normally need to contact the lender and ask it to investigate your concerns. As such it may be quicker to write directly to the lender yourself. It will also save you having to write to all of the credit agencies that hold the information you think is wrong.

The General Data Protection Regulations requires that a data controller, (the organisation who processes and controls the data), ensures that data is kept accurate and up to date. As such, if there is inaccurate data on your credit file then in certain circumstances you may ask the Information Commissioner's Office to look into the matter. Therefore, if, after writing to the lender or the credit reference agency, you feel the information is still wrong, or you do not receive a reply, you may then wish to bring your concerns to our office. The relevant information can be found via the following link: <https://ico.org.uk/make-a-complaint/>

## **SAR**

The right to access 'personal information' under the General Data Protection Regulations is known as 'Subject Access'. Although this office enforces the legislation we do not hold any personal information about individuals unless they have been in direct correspondence with us previously. If you believe information is held about you by other organisations, you should write to them directly.

I have provided a link to information about accessing personal information which is on our web site <https://ico.org.uk/your-data-matters/your-right-of-access/>

## **Parking**

Unfortunately this is a matter that we cannot help you with; you may be best placed to contact the company who issued the parking charge notice. From the correspondence you have enclosed it is likely this is [ ]. I have included their contact details below: [ ]

### **General misdirected**

Unfortunately this is a matter that we cannot help you with; you may be best placed to raise your concerns with [ ]. You can find the contact information for [ ] through this link [ ].

### **SkyDrive/Attachments which cannot be opened**

Unfortunately we are unable to open files sent to us in this [format/way]. To enable us to process your [concern/enquiry], please could you resend your email with the complaint form as an attachment (saved as a .doc, .docx, .pdf or .odf file).

### **Misdirected with disclosure of personal data to ICO**

If the misdirected case includes an inappropriate disclosure of PD from the sender, discuss this with an LCO\*

## **PA&DPCS - DS and DC templates**

### **100-year retention on the Police National Computer**

#### **Internal Overview for case officer:**

The force will need to justify the necessity and proportionality of the retention of the data and how this complies with the third and fifth data protection principle. Forces will be following the NPCC national retention policy<sup>1</sup>. Outcome type, category of offence and the time passed since the event will impact the proportionality of the retention.

Case officers should initially review the criminal records [knowledge pack](#) in the first instance before providing an outcome. Each case needs to be assessed on its individual merits, considering whether the case relates to an arrest only event where no further action was taken, or an overturned conviction. Time passed since the record was created should also be considered by the force.

Please note, while ACRO processes requests for deletion of records from the Police National Computer (PNC), it is the police force which submits the record to the PNC which is considered the responsible party. For this reason an outcome should be made in relation to the police force rather than ACRO.

Consider closing as 'Good practice advice provided'.

Note: Some of the paragraphs below provide standard wording. Please note that text in *italics* may need to be amended to fit the individual case and assessment.

The case reference should be referred to the intelligence department for monitoring<sup>2</sup>, and recorded as a 'hot topic', please consult the team manager for further information.

#### **DS template**

Dear **DS**

Thank you for the data protection concern you raised about **DC** and the way it has processed your sensitive personal data.

---

<sup>1</sup> [Microfiche Library \(publishing.service.gov.uk\)](http://Microfiche Library (publishing.service.gov.uk))

<sup>2</sup>

## Concern raised with us

You are concerned that **DC** has declined your request to remove its record relating to your arrest/attendance at **XXXX** Police Station/conviction from the Police National Computer ("PNC"). We note that no action was subsequently taken against you/your conviction was subsequently overturned.

We understand that **DC** has declined this request in line with national guidance which determines that the record should be retained until you are deemed to have reached 100 years of age.

## Our view

*In light of **DCs** justification for retaining your personal information, we **do not** at this stage consider its retention locally or on the PNC represents a breach of **DC's** obligations under the Data Protection Act 2018 ('the DPA').*

We accept that it may be necessary for forces to retain information for a certain period of time in case further evidence comes to light, or if the information has ongoing intelligence value in relation to future criminal behaviour (for example, in situations where it is important to understand a pattern of behaviour when deciding on an appropriate policing response).

However, we are concerned more generally with the blanket application of a 100 year retention period to all PNC data which includes a vast spectrum of information, from previous convictions to non-conviction outcomes (referred to as 'event history'), which will include acquittals, discontinuances and 'no further action' disposals.

We recognise that **DC** is following national guidance, but we have concerns over the proportionality of the blanket application of a 100 year retention period and the lack of a review process for all PNC records. We are engaging with the National Police Chiefs' Council ('NPCC') to review the application of this policy around the necessity to retain some event history records.

While **DC** is bound by national guidelines in terms of the PNC retention guidelines, as a controller, DC should ensure compliance with the Data Protection Act 2018 (DPA) which requires periodic reviews to take place to ensure ongoing retention of personal data is necessary. We will be providing advice to **DC** to ensure they have mechanisms in place to provide meaningful review of the information held to ensure that the ongoing retention of records on the PNC complies with data protection law.



## Next steps

Please be advised that matters such as whether the allegation was suitably investigated or whether the arrest itself was appropriate fall outside the remit of the Information Commissioner's Office and may instead need to be considered under **DC's** internal complaints procedure or via the Independent Office for Police Conduct.

We keep a record of all the concerns raised with us about the way **DC** processes personal data. The information we gather from concerns may form the basis for action in the future where appropriate.

Yours sincerely

**NAME**

Case Officer

Information Commissioner's Office

Direct dial number: 0330 414 **6XXX**

## Feedback about our service

If you are dissatisfied with the service you have received, or would like to provide us with feedback of any kind, please let me know.

For information about what we do with personal data see our privacy notice (emails)

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice) (postal)

## **DC template**

Dear XXXX

We are writing to you because a concern has been raised with us by:

### **[COMPLAINANT DETAILS]**

**DS** has raised a concern with us that **DC** has *declined his/her* request to remove its record relating to *his/her arrest/conviction* from the Police National Computer ("PNC").

As we understand it, **DS's** record relates to *his/her arrest/conviction on DATE*, which we note *resulted in no further action being taken against him/her/which was subsequently overturned*.

We understand that DC has *declined* this request in line with national guidance which determines that the record should be retained until DS is deemed to have reached 100 years of age.

We accept that it may be necessary to retain information for a certain period of time in case further evidence comes to light, or if the information has ongoing intelligence value in relation to future criminal behaviour (for example, in situations where it is important to understand a pattern of behaviour when deciding on an appropriate policing response).

However, we are concerned with the blanket application of a 100 year retention period to all PNC data which includes a vast spectrum of information, from previous convictions to non-conviction outcomes (referred to as 'event history'), which will include acquittals, discontinuances and 'no further action' disposals.

We recognise that DC is following current Record Deletion Policy of the National Police Chiefs' Council ('NPCC') but we have concerns over the proportionality of blanket application of a 100 year retention period and the lack of a review process for all PNC records.

[If DC has reviewed and considered the deletion request] - *We also acknowledge that DC has considered DS's request for early deletion under the current NPCC Record Deletion Policy.*

### **Action required**

Our underlying concern relates to the proportionality of national retention periods for PNC records. We recognise that DC does not own this policy and may not be in a position to unilaterally review it. With that in mind, we intend to deal with this matter at a strategic level with the NPCC in order to review both the overarching national retention policy and the Record Deletion Policy.

While DC is bound by national guidelines in terms of the PNC retention guidelines, as a controller, DC should ensure compliance with the Data Protection Act 2018 (DPA) which requires periodic reviews to take place to ensure ongoing retention of personal data is necessary. DC should ensure there are mechanisms in place to provide meaningful review of the information held to ensure that the ongoing retention of records on the PNC complies with the third and fifth data protection principles.

### **Next steps**

We keep a record of all the concerns raised with us about DC and will take these into account if more are received. The information we gather from concerns may form the basis for action in the future where appropriate.

Yours sincerely

**NAME**

Case Officer

Information Commissioner's Office

Direct dial number: 0330 414 6XXX

For information about what we do with personal data see our privacy notice (emails)

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice) (postal)

# PADPCS AND THE CHILDREN'S CODE

INFORMATION ABOUT THE IMPACT OF THE AGE APPROPRIATE DESIGN CODE  
(AADC) ON PUBLIC ADVICE AND DATA PROTECTION COMPLAINTS

**ico.**  
Information Commissioner's Office



children's  
code



The infographic features a blue gradient background with white circuit-like lines and nodes. On the left, the title 'THE CHILDREN'S CODE' is displayed in white. On the right, four rounded rectangular boxes contain key information about the code, with each box having a different shade of blue or green.

## THE CHILDREN'S CODE

Introduces 15 standards for information society services (ISS)

Organisations need to conform from 2 September 2021

Designed to protect children from **within** the digital world, not **from** it

First code of its kind in the world, it has already had a global influence

## THE STANDARDS

Best interests of the child	Online tools for children to exercise their rights and report concerns	Connected toys and devices	Age appropriate application	Parental controls
Detrimental use of data	Geolocation	Policies and community standards	Default settings	Nudge techniques
Data minimisation	Profiling	Transparency	Data sharing	Data protection impact assessments

# WHAT DOES THIS MEAN IN PRACTICE?



No nudge techniques



Age appropriate information



Geolocation off by default



Online tools for children to request deletion



Turn off profiling by default  
eg no unwanted ads



## WHY DO WE NEED A DIFFERENT PROCEDURE?

Complaints about the Children's Code will be referred to Operation Valency.

As a new code of practice, it is important to gather information quickly to help support organisations and deepen our understanding of the type of concerns that may arise following its introduction.

If a complaint from a child waits in a queue for a few months, this may mean that their complaint will not be resolved for a long time. It could have a big impact on a child's life while waiting for the outcome.

It is in the best interests of the child to look at these without delay.

It is very unlikely, but if a complaint contains a safeguarding disclosure, we may need to report this to an appropriate body.

If a child is at immediate risk we can contact the police. Waiting in the queue could cause serious harm if the child thinks they have told someone who can help.





## IMPACT ON LIVE SERVICES AND SOCIAL MEDIA

Increase in helpline calls and live chats from parents and civil society groups

Children may contact us directly, this is more likely to be via live chat or social media

Media coverage may increase the volume of these types of calls and contacts

Increased publicity may result in **misdirected** contact

## IMPACT ON ENQUIRIES

We may get enquires about the code or from children

Should be handled within the normal service standards timescales

Send details about any code related issues to

## IMPACT ON COMPLAINTS

Complaints solely relating to the code and complaints directly from children will be identified at sift

The case will be created and referred to

[REDACTED]

Complaints raised on behalf of children will be handled as normal

If a complaint from a child is picked up at a later stage, please refer it to the above email address

Complaints relating to the code can be referred to

[REDACTED]

## THINGS TO CONSIDER

Normal procedure for providing advice to children

Avoid jargon or explain it clearly


Signpost clearly to help children exercise their rights or to complain

Direct individuals to raise their concerns about the code with the organisation first

Complaints can be taken from children via live services and social media but we still need evidence

If you aren't sure if they are under 18, you can ask

Please complete the wrap! The more we know about the issues being raised, the more guidance we can provide



## THINGS TO LOOK OUT FOR

Obvious and direct references to the Children's Code, Age Appropriate Design Code, AADC or the standards

Direct or indirect references to the age of the customer eg my mum/dad/teacher

Updates on ICON

Current themes emerging: Private accounts by default including who can see social media posts, geolocation, targeted advertising to kids, etc.



## ORGANISATIONS AND SECTORS OF INTEREST

Some organisations have already been highlighted as falling under the Code in the media including TikTok, Instagram, Facebook, Google and YouTube (Kids)

Complaints from civil society groups: 5Rights Foundation, Privacy Matters, Open Rights Group

Sectors that are more likely to include complaints from children: DP1 - Schools, Education Technology, DP3 – Social Services, DP5 – Search Engines, Social Media, DP6 – Foster Care, Health

## WHAT NEXT?

- We will continue to provide updates and information about the code
- We will focus on relevant/current issues
- Contact Karen Bolton or Catherine Heverin with any queries

The Governor  
HMP

15 March 2019

Dear Governor,

I enclose a letter from the Information Commissioner's Office, which is being sent under the "Confidential Access" procedure.

I would be grateful if you could arrange for the enclosed correspondence to be delivered to the named recipient unopened.

If you have any queries, please contact me as below.

Yours sincerely,

Name  
Case Officer  
The Information Commissioner's Office

**Contact details:**

**Tel. xxxx xxx xxxx**

**Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF**



**Case Reference Number IC-\*\*\*\*\*-\*\*\*\*\***

Dear

I am writing further to your correspondence about XXXX.

I note from your correspondence that you are unhappy with **my response/ the outcome of your case.**

The matters you have raised will be passed to a **manager/reviewing officer** who will review your case and respond within 30 days. If the **manager/reviewing officer** is unable to send a full response within that timeframe, they will let you know what is happening and when you will receive a full response.

Yours sincerely,

## Template letter - RCC complaint not upheld

updated Aug 2020

### Case review response – complaint not upheld

This letter should be used when responding to a case review. Further detail may be included to address the specifics of the complaint and to explain the decision.

.....

Dear xxx

I am writing further to your request of [date] in which you have asked us to review the handling of your data protection complaint.

Your complaint has been passed to me for consideration and my role as a reviewing officer is to look at what we have done and why. Although I may not necessarily respond separately to each of the points you have raised I have:

- reviewed the information relating to your data protection complaint and considered the points you have raised;
- considered whether the complaint was dealt with reasonably;
- considered whether the matter was handled in line with our casework processes; and
- considered whether there are any outstanding matters for us to pursue.

### Your complaint and our review

I understand we have investigated your data protection complaint (about xxx) and you're unhappy with/concerned about [the outcome/the way it was handled/our decision not to take further action].

I have considered the points you have raised and have also reviewed the relevant information we hold about your case. I am satisfied that [case officer] dealt with your complaint appropriately and in line with our case handling procedures.

In this case [case officer] explained the reasons for [his/her] view in the letter of [date]. Having reviewed the matter, I am satisfied that [case officer] dealt with your complaint appropriately. As such this is not something that we intend to pursue further.

[xxx] further detail can be added to address the complaint or explain the decision

## Next steps and your options

Part of the Information Commissioner's Office (ICO) role is to consider complaints from people who believe there has been an infringement of the data protection law.

Under data protection legislation (Section 165 of the Data Protection Act 2018) we must investigate a complaint to an appropriate extent, and inform you of the outcome. Part of this process includes considering whether further action is necessary or appropriate, in line with our [Regulatory Action Policy](#).

If we think an organisation has not complied with its obligations we can give advice and ask them to solve the problem. Our main aim is to improve the information rights practices of organisations, where there is an opportunity for us to do so.

A case review is the final stage of the ICO's case handling process which means that we won't consider this complaint further. However I recognise that you may continue to disagree with our view.

It may be helpful to explain that you are entitled to take your own cases to court under data protection legislation, irrespective of our decision. The ICO has no role in individual applications to the court, so if you wish to pursue this option, you may wish to seek private legal advice.

Alternatively if you believe that the ICO has provided you with a poor service, or if you believe we have not treated you properly or fairly then you may be able to complain to: **The Parliamentary and Health Service Ombudsman (PHSO), Millbank Tower, Millbank, London, SW1P 4QP.**

All complaints to the PHSO must be made through an MP. If you require further information about the PHSO, you can call its helpline on 0345 015 4033.

Yours sincerely

Name of case officer  
Job title  
Information Commissioner's Office  
Direct dial telephone number

Please consider the environment before printing this email

For information about what we do with personal data see our [privacy notice](#)

I write in response to the concerns you raised with our office on [DATE] . My name is [NAME] and, as a Team Manager at the Information Commissioner's Office (ICO), your concerns have been passed to me to review and respond to. I have considered your correspondence and document my findings below.

## **Introduction**

## **My Findings**

## **Next Steps**

If you still believe that we have provided you with a poor service or if you believe we have not treated you properly or fairly then you may be able to complain to:

**The Parliamentary and Health Service Ombudsman (PHSO),  
Millbank Tower, Millbank, London, SW1P 4QP.**

All complaints to the Ombudsman must be made through an MP. I would advise you to first call the Ombudsman's Helpline on **0345 015 4033** or visit their website to see if they are able to assist you further:

<https://www.ombudsman.org.uk/>

If, however, your complaint relates to the way in which we have interpreted the law then the Ombudsman cannot help you. If you want to challenge our interpretation of the law, you should consider seeking legal advice.

For information about what we do with personal data see our [privacy notice](#).

Yours sincerely

XXXX  
Team Manager  
Tel. 0330 414 6XXX

## Template letter - RCC complaint upheld

updated Aug 2020

### Case review response – complaint upheld

This letter should be used when responding to a case review. Further detail may be included to address the specifics of the complaint and to explain the decision.

.....

Dear xxx

I am writing further to your request of [date] in which you have asked us to review the handling of your data protection complaint.

Your complaint has been passed to me for consideration and my role as a reviewing officer is to look at what we have done and why. Although I may not have responded separately to each of the points you've raised, I have:

- reviewed the information relating to your data protection complaint and considered the points you have raised;
- considered whether the complaint was dealt with reasonably;
- considered whether the matter was handled in line with our casework processes; and
- considered whether there are any outstanding matters for us to pursue.

### Your complaint and our review

I understand that we have investigated your complaint [about xxx] and you're unhappy with/concerned about ... [the outcome/the way it was handled/our decision not to take further action].

I've considered the points you have raised and have also reviewed the relevant information we hold about your case. I understand how [case officer] reached their view, but I agree that this warrants further consideration.

As such we will ... [outline what steps you will take and what the complainant can expect]

### Next steps and your options

Part of the Information Commissioner's Office (ICO) role is to consider complaints from people who believe there has been an infringement of the data protection law.

Under data protection legislation (Section 165 of the Data Protection Act 2018) we must investigate a complaint to an appropriate extent, and inform you of the outcome. Part of this process includes considering whether further action is necessary or appropriate, in line with our [Regulatory Action Policy](#).

If we think an organisation has not complied with its obligations we can give advice and ask them to solve the problem. Our main aim is to improve the information rights practices of organisations, where there is an opportunity for us to do so.

As outlined above we will do **xxx** which I hope will resolve your complaint.

However I would also add that if you remain dissatisfied with this course of action you are entitled to take your own cases to court under data protection legislation, irrespective of our decision. We have no role in individual applications to the court so if you wish to pursue this option, you may wish to seek private legal advice.

Alternatively if you continue believe that the ICO has provided you with a poor service, or if you believe we have not treated you properly or fairly then you may be able to complain to: **The Parliamentary and Health Service Ombudsman (PHSO), Millbank Tower, Millbank, London, SW1P 4QP.**

All complaints to the PHSO must be made through an MP. If you require further information about the PHSO, you can call their helpline on 0345 015 4033.

Yours sincerely

Name of case officer  
Job title  
Information Commissioner's Office  
Direct dial telephone number

Please consider the environment before printing this email

For information about what we do with personal data see our [privacy notice](#)

## **Service adjustment record**

Please complete this form if you require a reasonable adjustment and include as much information as possible. If you require any further assistance then please call our helpline 0303 123 1113 or email us [icocasework@ico.org.uk](mailto:icocasework@ico.org.uk).

**Customer name:**

**Address:**

**Email:**

**Telephone no:**

**Case reference:**

**Reason for adjustment:**

**Nature of adjustment:**



## Case Reference Number -

Dear

The Information Commissioner's Office ('ICO') has received a concern that you may be operating a CCTV system in a way that requires you to comply with the Data Protection Act 2018 (the DPA).

The ICO is a UK independent regulatory authority reporting directly to the UK Parliament. The Commissioner enforces and oversees the DPA.

Our purpose is to improve information rights practices. For further information on who we are and what we do, you may wish to visit our website at [www.ico.org.uk](http://www.ico.org.uk).

### Why we are contacting you

The use of CCTV for limited personal and household purposes is generally exempt from the requirements of the DPA.

However, a court case (*Ryneš*) concluded that where a surveillance camera faces outwards from an individual's private domestic property and captures images of individuals **beyond the boundaries** of their property, the recording cannot be considered to be for a purely personal or household purpose.

The use of CCTV in such circumstances is not exempt from the DPA and you should use the system in line with the guidelines enclosed.

### Next steps

If you are operating CCTV which captures footage outside the boundaries of your property you should refer to the information provided and take any steps required to ensure your compliance with the DPA.

The easiest way of doing this is to consider repositioning any cameras to operate inside your boundary so that they are exempt from the DPA altogether.

We now consider this matter to be closed and do not require any correspondence or confirmation from you in response to this letter.

Yours sincerely,

**Information Commissioner's Office**

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

[Name]  
[Address line 1]  
Address line 2]  
Postcode

Date as postmarked

**Case Reference Number #####**

Dear [NAME],

I write in response to your correspondence about the CCTV operated by your neighbour.

Our aim is to improve information rights practices. We do this by taking an overview of all concerns that are raised with a view to improving compliance with the Data Protection Act 2018 (DPA).

The DPA **does not prevent** the use of CCTV cameras. Instead it provides a framework within which they can be operated.

In relation to your neighbour, the DPA only applies if personal data is being captured beyond the boundaries of the individual's private property.

**Next steps**

We will contact your neighbour informing them of the requirements of the DPA, and request that any necessary steps are taken to ensure they comply. **The ICO cannot instruct your neighbour to remove or reposition their CCTV cameras.**

If you feel harassed or intimidated by your neighbour using CCTV, you may wish to speak to your local police officer.

There is separate legislation that may help in resolving your concerns, such as the Protection from Harassment Act 1997, the Public Order Act 1986 and the Anti-Social Behaviour (ASB) – Crime and Policing Act 2014. You should advise the police that we directed you to them.

We have now fulfilled our statutory obligations. Should you have further concerns you may wish to seek independent legal advice.

Yours sincerely

Xxx

DATE

**Case Reference: RFA0XXXXXX**

Dear XXX,

Thank you for your correspondence regarding XXXXXX.

**The ICO's role**

Part of our role is to consider complaints from individuals who believe there has been an infringement of their data protection rights.

**Concern raised with us**

You are concerned that a former employee of your organisation has processed personal data in order to contact your clients for their own business.

This matter relates to section 170 of the DPA 2018. This part of the Act relates specifically to the unlawful obtaining of personal data.

**Our view**

As the main purpose of the DPA is to protect the rights of individuals and not to protect the commercial interests of businesses who hold the information, we would not look to pursue this matter at this time as we have not been provided with any evidence of detriment to the data subjects (the clients).

Based on the information you have provided, we would consider this concern to be a 'business to business' matter which would be covered by the terms of contracts of employment.

Should any of the clients themselves raise a concern about how their personal data has been handled then we would reconsider the case. However, this would be in respect of XXX's wider data handling practices and the potential detriment to data subjects, rather than the impact upon the business of XXX.

**Next steps**

We would always suggest that businesses consider including post-employment restrictive covenant clauses in employment contracts, to clarify who controls the



Information Commissioner's Office

personal data and to set requirements as to what happens when employees go to work for another business.

Businesses may always seek redress in the courts regarding such matters and any breach of a restrictive covenant clause would add weight to any such case. If this is something that you are interested in pursuing we would recommend that you obtain independent legal advice.

Thank you for bringing this matter to our attention and I hope that the above information has helped to clarify the role of the ICO. Should you wish to discuss the case any further then please feel free to contact me. If you are responding via email, you can forward your response to our [casework@ico.org.uk](mailto:casework@ico.org.uk) email address with the above case reference in this format [Ref. RFAXXXXXX] in the subject line.

Yours sincerely,

Case Officer

Information Commissioner's Office

Direct Dial:

For information about what we do with personal data see our [privacy notice](#)

**Contact Record – Case closed as a result of telephone contact**

**\*Remember to do your security check with customer and only leave a voicemail message if appropriate\***

Date & time of call	
Details of call	

Please complete this document after the call, remembering to record all information relevant to the case, and save as a document on the case. The document should be entitled '**telephone closure case record**'.

## Escalation letter to CEO or DPO

This escalation letter should be sent to a CEO (or DPO) if a customer contacts us to say that they haven't heard anything following an accountability letter. You should carry out checks to make sure that the new contact details are correct. If you can't verify the contact details, or the company doesn't have a CEO or DPO, you can write to the person that you initially contacted.

You can send the DS a copy of this letter providing you take steps to ensure there are no inappropriate disclosures. To reduce this risk you shouldn't automatically copy the DS into this email. You will need to use your judgement about whether you can send a copy as an attachment.

.....

Dear CEO

The attached email was sent to you/your DPO on [insert date]

Your customer has been back in touch with us to say that their concerns haven't been addressed and that this matter is still outstanding.

We therefore expect you to put this right by contacting your customer within the next **seven** days. A record of this complaint and how it has been dealt with will be kept on file.

Yours sincerely

Case Officer



I am writing from the Information Commissioner's Office ('ICO'), because we have received a data protection complaint about the information rights practices of the following organisation:

**DC name**

**DC address**

**Any other relevant information about the DC without disclosing any personal data of the DS and their complaint.**

We would be grateful if you could kindly confirm if we have contacted the correct organisation and if so, provide the name and contacts details of the individual best placed to handle this complaint within your organisation.

Once we have received confirmation of the above, we will provide further details of the complaint.

We would appreciate if you could provide this information within **seven calendar days**.

Dear

Thank you for your **email/letter** of XXXXX.

## **OR**

The Information Commissioner's Office (ICO) is writing to you because we have received a complaint from **XXXXXXXXXX** that you **[INSERT BRIEF DETAILS OF COMPLAINT]**

## **What we do**

Part of our role is to consider complaints from individuals who believe that there has been an infringement of the data protection law.

The Data Protection Act 2018 requires us to investigate a complaint to the extent we feel is appropriate and to inform the individual of the outcome.

## **Our view**

We have considered the issues raised with us. Based on the information provided, it is our view that **you have/have not** infringed your data protection obligations. This is because:

**Below is a non-exhaustive list of some of the infringements- use suggested paragraph folder to expand. Use links to website also.**

- **You have/have not properly responded to the subject access request**
- **You have/have not properly responded to the request for rectification.**
- **You have/have not properly responded to the request for erasure.**
- **You have/have not properly responded to the request to restrict processing. click here for paragraphs about**
- **You have/have not properly responded to the request to object to processing. You have/have not properly responded to the request for portability.**
- **You have/have not kept personal information securely You have/have not inappropriately disclosed personal information to a third party**

## **Further action required**

You should now take steps to improve your information rights

practices. You should ensure that ... [details relevant steps the organisations should take to address the infringement. For example see below]

- All staff attend mandatory training which is routinely tested and refreshed;
- All policies and procedures are updated and revised to reflect the new obligations placed on controllers and processors under the GDPR / DPA18; and
- All data processed by [insert DC/DP] is subject to appropriate organisational and technical controls with regards to its security.

### **What we will do**

We keep a record of all the complaints raised with us about the way you process personal information.

The information we gather from complaints may form the basis for action we may take in the future to ensure you meet your information rights obligations.

Yours sincerely

Name of case officer  
Job title (but not department name)  
Information Commissioner's Office  
Direct dial telephone number

If you would like to provide us with feedback of any kind, please let me know

### **ICO Statement**

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Any correspondence, letters, emails and notes of phone calls, may be considered for disclosure. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do. It should be noted, the ICO will not release any information unless we have the lawful authority to do so.

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice)

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link: [Complaints and concerns data sets | ICO](#).

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at [accessicoinformation@ico.org.uk](mailto:accessicoinformation@ico.org.uk). We will only agree to this in limited circumstances where we are satisfied that the interests of the parties involved would override the ICO's obligations to publish this information.

The Information Commissioner's Office (ICO) has received a complaint about the way your organisation processes personal data. **X has complained that [insert brief details of the complaint received. You may wish to provide relevant documents].**

The ICO considers complaints from individuals who believe there has been an infringement of the data protection law. We are required to investigate a complaint to the extent we feel is appropriate and inform the complainant of the outcome under Section 165 of the Data Protection Act 2018.

In order to resolve this complaint, you must take the following steps:

- **Review the complaint outcome**

You should look again at the issues raised by your customer.

You should consider whether there is any further action you can take that may resolve this complaint.

If you believe you have complied with the law, you should explain your reasoning to us.

- **Provide us with further information**

You should also provide us with the following details: **[THIS IS NOT AN EXHAUSTIVE LIST BUT GIVES A GOOD IDEA OF THE ADDITIONAL INFORMATION WE CAN REQUEST]**

- how you have handled this complaint/request for information/any other individual right in this case;
- (If SAR) any information you withheld and why you did so;
- **[ADD ANY ADDITIONAL RELATED ISSUES];**
- any safeguards you have in place to help you handle personal data properly, particularly about this specific matter; and
- any steps you have taken to add to or strengthen these safeguards.

You must send us your response as soon as possible and in any event within **\*\* days**. If you are unable to provide a response within this timeframe, please contact me directly.

If you do not provide the information we have requested, we will either base our decision on the information available or consider issuing an Information Notice.

- **Review your practices**

Our website contains advice and guidance about the processing of personal data and your organisation's obligations under the data protection law. I recommend that you review the information on our website before finalising your reply.

If you need to discuss this further or have any queries, you can contact me on the number below.

Yours sincerely

Name of case officer  
Job title (but not department name)  
direct dial telephone number

### **ICO statement**

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Any correspondence, letters, emails and notes of phone calls, may be considered for disclosure. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do. It should be noted, the ICO will not release any information unless we have the lawful authority to do so.

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice)

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link: [Complaints and concerns data sets | ICO](#).

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at [accessicoinformation@ico.org.uk](mailto:accessicoinformation@ico.org.uk). We will only agree to this in limited circumstances where we are satisfied that the interests of the parties involved would override the ICO's obligations to publish this information.

Dear

Thank you for submitting a complaint about the processing of your personal information. We understand how important this is to you.

### **What we do**

When we receive a complaint like yours we start by looking at how the organisation has dealt with it. It's important to us that organisations earn your trust by showing that they've done all they can to deal with your data protection concerns.

The DPA 2018 also requires us to investigate a complaint to the extent we feel is appropriate and to inform you of the outcome.

We have considered the issues that you have raised with us and based on this information, it is our view that there is more work for the organisation to do.

We have therefore raised your complaint with the Chief Executive, via the Data Protection Officer, explaining that we want them to work with you to resolve any outstanding matters.

I have attached a copy of the letter we have sent to them.

### **What we expect the organisation to do**

We think that the organisation may want to look again at the issues that you have raised.

If the organisation believes they have complied with the law, we expect them to clearly explain that to you.

If something has gone wrong, we expect them to work with you to put things right and to learn from their experiences and improve their practices.

We have allowed the organisation 28 days to consider the issues that you have raised and to consider next steps in your case.

We expect they will be in contact with you in due course.



We have closed your case and don't intend to take any further action at this time.

Thank you for bringing this matter to our attention.

Yours sincerely,

NAME

Case Officer

Information Commissioner's Office

Tel: 0330 XXX XXXX

### **Feedback about our service**

If you think we should have done something differently in how we have handled your concerns, or how we have treated you, please tell us.

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice).

Dear [XXXX]

Thank you for submitting a complaint about [insert brief details of the complaint received]. We understand how important this is to you.

### **What we do**

Part of our role is to consider complaints from individuals who believe there has been an infringement of the data protection law.

The Data Protection Act 2018 requires us to investigate a complaint to the extent we feel is appropriate and to inform you of the outcome.

We use complaints to build up a picture of an organisation's information rights practices so that we can identify and target poor performing organisations. Details of the [action we have taken is available on our website.](#)

### **Our view of your complaint**

We have considered the issues that you have raised with us and based on this information we have contacted [XXXX]. We have asked them to give us further information about your complaint and their information rights practices.

### **What will happen next**

We will write to you again when we have received their response to let you know the outcome of your complaint.

If you would like to discuss this further, please reply directly to this email or call me on the number below.

Yours sincerely

Xxx

### **Feedback about our service**

If you think we should have handled your concern or treated you differently, please tell us.

For information about what we do with personal data, see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice).

**Update letter to DS – following non response to accountability letter**

This letter should be sent to a DS if they advise us that they haven't heard anything from a DC following an accountability letter.

.....

Dear xxx

Thank you for letting me know that your data protection concerns haven't been addressed. I have written to xxx to let them know that this matter is still outstanding and advised them to contact you within the next **seven** days. I hope that this will resolve matters but if you do not hear back from them please do let me know.

Yours sincerely

Case Officer

Dear

Thank you for submitting a complaint about the processing of your personal information. We understand how important this is to you.

We have considered the issues you have raised but have not been able to decide whether there has been an infringement of data protection law. This is because we need to see the evidence to support your complaint.

There are two options for what you need to do next, depending on whether you have already complained to the organisation:

- **If you have not yet complained to the organisation**

If you have not yet complained to the organisation, we strongly recommend that you do so to give them the chance to put things right. We have information on [how to make a data protection complaint to an organisation](#) that may help you to do this.

We always want to allow organisations the opportunity to resolve matters with you and we expect that most cases will be resolved without our intervention. Organisations should work with you to explain how they have handled your personal data, and help you to exercise your rights properly.

- **If you have already complained to the organisation**

If you have received a final response from the organisation, and they have stated that they will not look at matters further, then please come back to us.

We need you to send us copies of letters or emails you've sent to the organisation explaining what your information rights complaint is. It is important that you include any final response that the organisation has sent to you.

Please quote the reference number at the top of this letter on any future correspondence about this matter.

We fully expect that most cases can be resolved without our intervention. We will now close this complaint. However, it will be revisited if you aren't able to get matters resolved and you send the supporting evidence we need.

If you require any further advice or assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Xxx

Investigation/enforcement referral letter for Public interest group cases

Dear

Thank you for your correspondence to the Information Commissioner's Office (ICO) in which you have raised a complaint about...

### **Next steps – further action**

Part of our role is to consider complaints from individuals who believe there has been an infringement of their data protection rights. Once a concern is raised with us, we record and consider it. In some cases, we collate further information on similar issues, looking at the concern alongside others raised about the organisation as well as other intelligence and information we may have about the organisation.

It is up to us to decide whether or not we should take further action in a particular case or against a particular organisation. We make these decisions based on the Regulatory Action Policy and our Information Rights Strategic Plan (both available on our website [www.ico.org.uk/about-the-ico/our-information/](http://www.ico.org.uk/about-the-ico/our-information/)).

**[OPTIONAL FOR PUBLIC INTEREST CASES** *In this case, as we have not received a complaint from an individual about the processing of their own personal data, it has been necessary to consider the extent to which our obligations to consider individual complaints applies, and if not, the other options available to us to take this matter further.*]

Due to the wide ranging and serious nature of the concerns you have raised, alongside other information we have regarding the organisations and sectors concerned, we have taken the decision to refer this case to Investigations with a view to taking further action in line with the Regulatory Action Policy.

Given the breadth of the issues raised in this and related cases, it is likely to be some time before any outcomes are reached. **[Check with INVESTIGATIONS re: updates before including:** *However, we will contact you to let you know the outcome as soon as we are able.*]

It is **[also]** likely that any outcomes will be published on our website.

Dear [XXXX]

Thank you for your complaint about [insert brief details of the complaint received]. We understand how important this is to you.

### **What we do**

Part of our role is to consider complaints from individuals who believe that there has been an infringement of the data protection law.

The Data Protection Act 2018 requires us to investigate a complaint to the extent we feel is appropriate and to inform you of the outcome.

### **Our view of your complaint**

We have considered the issues you have raised with us. Based on this information, it is our view that xxxxx **has/has not** infringed their data protection obligations. This is because:

Below is a non-exhaustive list of some of the infringements. Use suggested paragraphs folder to expand your explanation. Also use links to website as required.

- You **did/did not** receive an appropriate response to your subject access request.
- You **did/did not** receive an appropriate response to your request for rectification.
- You **did/did not** receive an appropriate response to your request for erasure.
- You **did/did not** receive an appropriate response to your request to restrict processing.
- You **did/did not** receive an appropriate response to your request to object to processing.
- You **did/did not** receive an appropriate response to your request for data portability.
- Your personal data was not kept securely.
- Your personal data was inappropriately disclosed to a third party.

**[IF NO INFRINGEMENT THIS SHOULD BE STATED AND ADVISED THAT WE WILL HOLD A RECORD OF THE COMPLAINT BUT NO FURTHER ACTION NEEDED].**

**[IF FURTHER ACTION REQUIRED]:**



## **What we expect the organisation to do**

We have written to xxxx about their information rights practices. We have told them they should now ensure that... [details of the relevant steps the organisations should take to address the infringement. **For example,** see below]

- All staff attend mandatory training which is routinely tested and refreshed;
- All policies and procedures are updated and revised to reflect the new obligations placed on controllers and processors under the GDPR; and
- All data processed by [insert controller/processor ] is subject to appropriate technical and organisational security measures.

## **What we will do**

We keep a record of all the complaints raised with us about the way organisations process personal information.

We use complaints to build up a picture of an organisation's information rights practices so that we can identify and target poor performing organisations. Details of the [action we have taken is available on our website.](#)

Thank you for bringing this matter to our attention.

### **[If necessary]**

You may have a right to an effective judicial remedy / right to compensation and liability.

If you are seeking personal redress or compensation for the way an organisation has dealt with your personal information, you need to pursue this independently through the courts or with an industry's own ombudsman or regulatory body.

The ICO is unable to assist you with this process. We therefore recommend that you seek independent legal advice, if you wish to pursue this course of action.

Yours sincerely

Xxx

### Feedback about our service

If you think we should have done something differently in how we have handled your concerns, or how we have treated you, please tell us.

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice).

## DS Chaser response

Dear [XXXX]

Thank you for your request for an update on your case.

The Information Commissioner's Office is dealing with a significant number of complaints at the moment which means it is taking longer than we would like to allocate your case to a case officer.

Your case was received on [XXXXXX]. In terms of our oldest cases, we are currently allocating cases received in [Month] 2022. We hope to be able to allocate your case in the next [XXX weeks], however this is only an estimate.

We know that when we receive a complaint the issue is important to you. Once your case is allocated, the case officer will contact you to explain what will happen next.

If you submit further correspondence before your case is allocated, it will be added to your case but it won't be reviewed until it is allocated to a case officer.

*[If it is obvious key information needed to progress the complaint has not been provided, LCO to add request for customer to provide missing info eg letter of authority, name of data controller. See [HTC template](#) for suggested wording.]*

We have lots of useful information about your individual rights on our website. You can view this by clicking [here](#). If you need advice on a new issue please call our helpline on 0303 123 1113 or use our live chat service.

Sent on behalf of  
Public Advice and Data Protection Complaints Service  
Information Commissioner's Office

For information about what we do with personal data see our [privacy notice](#).

**Unauthorised use of ICO logo – template for reporter**  
(please make Corporate Comms aware of any reports)

---

Dear [reporter's name]

Many thanks for contacting us and kindly bringing to our attention that **XXXXXXXXXXXX** are displaying our logo without permission.

Companies can say they are registered with the Information Commissioner's Office (or ICO), if they are, but as we are the UK's regulator for data protection, we think third parties using the ICO logo for this purpose could signal or imply that we have in some way checked or signed off their compliance with the Data Protection Act.

You may see it elsewhere but where it has not been authorised, we ask for it to come down.

You can see more information on [copyright and re-use of materials](#) on our website.

We will write to **XXXXXXXXXXXX** to ask that they remove our logo from any digital and/or printed marketing material with immediate effect. Thank you again for bringing this to our attention.

Yours sincerely,

NAME  
JOB TITLE  
DIRECT DIAL  
Information Commissioner's Office

## Warning letter – suggested wording

Dear XXXX

I am aware of the recent contact you have had with **CO/LCO** in our Public Advice and Data Protection Complaints Services.

During a telephone conversation on **[insert date]** you repeatedly used insulting and offensive language, calling **CO/LCO 'a \$£\*&^%'**.

The use of aggressive, threatening or abusive language, (including raising of the voice, swearing or shouting) which threatens or intimidates staff is not acceptable.

We aim to treat everyone we deal with fairly and with integrity and respect but we also expect similar consideration in return. No matter what your view of the ICO or its employees, we will not tolerate unacceptable or unreasonably persistent customer behaviour of this kind.

We may impose restrictions on your access to our services if it's necessary to protect our staff from unacceptable behaviour, as defined in our [managing customer contacts policy](#) and our [unreasonable and unacceptable behaviour policy](#). If we receive similar calls from you in future we will decide whether to restrict you from contacting us by phone.

Yours sincerely

Team Manager