# Information Governance E-Learning

|  |  |
| --- | --- |
| Document Name | Information Governance E-Learning |
| Author/Owner (name and job title) | Steven Johnston, Team Manager |
| Department/Team | Information Management Service |
| Document Status (draft, published or superseded) | Published (Current e-learning 2021 roll out) |
| Version Number | V3.0 |
| Release Date | 13/09/2021 |
| Approver (if applicable) | N/A |
| Review Date | 01/09/2022 |
| Distribution (internal or external) | Internal |

# Title: Information Governance at the ICO

Last modified at: Wed, 23 Dec 2020 11:50:16 GMT

Last updated by: Helen Fisher

Menu page introduction:

An important part of working with information is knowing how to handle it correctly. By developing good practices, we can avoid simple mistakes and help keep our information protected.

Work through each topic before you take the assessment.

Click or tap on the blocks below to get started.

Below are approximate timings to complete each section. It will not time out if you take longer and you do not have to complete it in one go.

## Page – 1 - Introduction

5 mins

### Introduction

Information is your business. Everyone at the ICO is responsible for keeping our information safe, protected and properly managed.

This course gives you basic principles to follow to ensure you fulfil your responsibilities. Look out for local procedures in your area.

This course will help you understand what our obligations are and what's expected of you.

We’ll help you continue to learn as our practices develop.

### Why is Information Governance important?

Customers, stakeholders and staff must be able to trust in the way we process our information. We are transparent about what we do and accountable for the way we process all of our information.

Our approach to good information governance is risk based, leading us to implement proportionate solutions.

Information is our currency.

1 Our mission is to uphold information rights for the UK public in the digital age.

We oversee information rights laws as the UK regulator and supervisory authority for the reformed data protection laws.

2 We're not just the regulator.

We're a controller for the purpose of data protection.

We're a public authority for the purpose of freedom of information, data protection and associated laws.

And we're a competent authority where we process personal information for the purpose of law enforcement.

We have the same obligations as the organisations we regulate.

We have to be a model of good practice, protect individuals’ rights and uphold the law.

3 Think about all the different types of information you handle at work. It might be information about the people you manage, the people who complain to us, or the people who make enquiries.

Protecting our information means we are accountable for it, respect people's rights to it, hold it securely and use it to help our decision making.

### ICO Confidential

Information Security

There is a specific obligation of confidentiality for the Commissioner and their staff in the Data Protection Act 2018. You need to be careful of what you tell people about our work. This obligation applies while you work for the ICO, and afterwards. Disclosing information you shouldn’t, could be a criminal offence – it is important you are aware of this and ask if you need advice.

\_graphic alt Series of images: In the pub, nuisance callers, commuting, at a conference, CCTV cameras

1 At the pub

"I’m in the pub with my friends, we’re talking about social media companies and how they use our information. I explain exactly what the social media companies have told the ICO so that my friends can better understand their position."

This is likely to be a breach of confidentiality and could be a criminal offence. Talking about the ICO to friends and family is perfectly acceptable as long as you don't reveal details given to the ICO by a third party – even if you’ve had access to the information to do your job.

2 Nuisance calls

"I’m dealing with a complaint about nuisance calls and the company doesn’t seem to understand what I want from them. I send them a copy of a response I’ve received from a similar company in a similar complaint to hurry them along."

This is likely to be a breach of confidentiality and could be a criminal offence. Sharing information from a third party without lawful authority is likely to damage relationships with stakeholders.

3 Commuting

"I’m on a train on the way home from a long day of meetings in London. I get a call from my manager who wants an urgent update. I give a detailed breakdown of the meetings and explain the position of our stakeholders and what I think we should do next. The carriage is busy."

This is likely to be a breach of confidentiality and could be a criminal offence. Divulging details of other organisations’ plans and views could damage relationships with stakeholders and make them less likely to be open with us.

4 Conference

"I’m at a conference and a senior member of staff from an organisation we deal with a lot, asks me about a high profile case. It’s recently been confirmed in the media that the ICO is investigating. I don’t want to seem rude."

In this case, you can avoid a breach. You can engage in conversation. You can go over what’s in the public domain and, for example, agree it’s a high profile and important issue. You could discuss the issues at play, in principle, but explain there’s a limit to what you can say about the specific case.

5 CCTV

"My neighbour tells me she’s made a complaint to the ICO about another of our neighbours’ use of CCTV and she says it’s taking a while to reach a conclusion. I’m really keen to know what happens because I’ve also been concerned about the cameras. I know the complainant’s full name and address so I think I’ll have a look on the casework management system and see where it’s up to – then I can let her know."

This is likely to be a breach of confidentiality and could be a criminal offence. You might be able to search for the case but you should not look at cases, or disclose information about them for your own personal reasons.

### How this course will help you

Is information important?

This course is a practical support designed to help you protect our information at the ICO. It will give you the tools you need to follow good practice and comply with the legislation we oversee.

In the topics that follow, you'll find out:

• How to manage and account for the information we create and store

• How to spot and handle requests for information

• What you can do to keep all our information secure

We won't be able to cover every situation you might find yourself in, but we'll certainly tell you where you can find out more. And remember, if you're not sure about anything then please ask.

## Page – 2 – Accountability

15 mins

### Managing our information

Information is our most valuable asset, so we have to look after it and be accountable for it. We all need to take personal responsibility for managing the information we create and use on a daily a basis.

We demonstrate our accountability by keeping good records of the work we've done, the decisions we make and how we comply with the law.

Keeping good records means we are always able to find what we need, understand them and maintain the integrity of our information.

### Why keep good records?

Look at the following scenario and answer the questions that follow.

1 "I've been working with the ICO for three years now.

I mainly deal with FOI requests but sometimes I have to find information to support our response to parliamentary questions, court orders or public inquiries."

2 "It’s Wednesday today. On Monday, my manager asked me to find information for a court order. The deadline was two weeks today.

Should be straightforward, right? Well, so I thought until I started. I soon discovered that the last person who'd worked on this case had left the ICO a few months back.

We keep all our case files on our casework system so that was the first place I looked."

3 "Unfortunately, I couldn't find anything to help me. There were a few files on a case which the name suggested might be relevant. However, the files had filenames like 'Document 2' and 'Notes made on the 2nd March', which didn't tell me much and didn't follow our file-naming conventions.

And when I opened these documents, they were just vague notes from a meeting. The notes were very brief and there wasn’t a clear record of the decisions made in the case. Also there wasn't anything to tell me where else to look. A pretty incomplete picture of the case!"

4 "I thought that maybe the information had been kept somewhere else, and the case officer hadn't got round to saving them to the right corporate system. A colleague seemed to think there were some documents still left in the case officer's locker and also recalled some meeting minutes being circulated via Microsoft Teams in March.

I did find a bundle of papers in the locker eventually but with only a day to spare! I couldn’t find the meeting minutes and I’m really worried our records about this case are incomplete."

### What went wrong?

Why couldn't your colleague find the information they needed?

1 They were looking in the wrong place

2 The information wasn't saved where it should have been

3 They didn't know what they were looking for

4 The documents were poorly file-named

5 When the case officer left, they didn’t tidy up their records

6 Documents were left in a personal locker

feedback correct That's right.

The case officer hadn't kept good and complete records on our corporate systems. This meant that colleagues struggled to find what they needed and we could end up in breach of a court order. Additionally, if the case files had been lost then this could be a breach of security. Remember applications such as Microsoft Teams are great for collaboration but are not appropriate to store information long term. You should always move your records to our casework systems or SharePoint EDRM as soon as possible. You should allocate yourself time to do this on a regular basis.

\_ feedback incorrect

That's not quite right.

The case officer hadn't kept good and complete records on our corporate systems. This meant that colleagues struggled to find what they needed and we could end up in breach of a court order. Additionally, if the case files had been lost then this could be a breach of security. Remember applications such as Microsoft Teams are great for collaboration but are not appropriate to store information long term. You should always move your records to our casework systems or SharePoint EDRM as soon as possible. You should allocate yourself time to do this on a regular basis

### Roles and responsibilities

We have a Privacy and Information Risk Management Network in place across the business to help us manage risk so that the above scenario stays as 'just a story' and does not become a reality. Our framework gives a number of individuals’ key responsibilities for managing information and its associated risks. Let's have a look at who they are.

1 Paul Arnold

Paul Arnold, our Deputy Chief Executive is our Senior Information Risk Owner (SIRO).

Our SIRO is responsible for information risk across our business.

2 Louise Byers

Because we're also a public authority, we have a Data Protection Officer (DPO) Louise Byers.

Our DPO, supported by a number of compliance teams, is responsible for our own data protection compliance. This includes internal policy and advice.

3 Information Asset Owners (IAO)

Our Information Asset Owners (IAOs) are the directors of services. They have a responsibility to review the risks to the confidentiality, integrity and availability of their information assets, including those in their delivery chain. They are mostly responsible for the protection of information held on ICT networks and also for the management of other assets such as paper records.

4 Information Asset Managers (IAM)

body Our Information Asset Managers (IAM) are our Heads of Department. They work with the IAO to minimise information governance risks within their teams. They help to ensure their teams are correctly following our procedures and guidance.

5 Local Information Management Officer (LIMO)

body Our Local Information Management Officers (LIMO) support the IAO and IAM. They act as the departmental contacts for any questions you might have about information management matters. They liaise with our central Information Management Service and represent their department at our Information Management Community meetings

6 Local Asset Administrators (LAA)

We also have Local Asset Administrators (LAA) where they are required. LAAs support local information management by keeping up with important administrative tasks, such as keeping asset registers up to date.

7 SharePoint EDRM Site Owners

body Our Site Owners have a responsibility to manage our digital information assets within SharePoint EDRM. They act as the departmental contact for any questions you might have about SharePoint EDRM.

8 All responsible

Whilst these roles have specific responsibilities, we are all responsible for making sure we manage our information properly.

### What role do you play?

Good information management helps you work better with your colleagues, and find the information you need to do your job. We'll look at each of these practices in a bit more detail throughout the topic.

1

Save information in the right place so others can find it

• Is all the information you handle saved in the correct place?

• Have you correctly 'checked in' your documents to SharePoint EDRM so that others can see them?

• Can you find it easily? Could others find it easily if they didn't have you to ask?

• Is the storage suitable for the nature of the information? For example, is all your casework saved on the casework system?

2

Storing important information

• Make records of significant activities/actions or decisions

• Make sure your records are complete

• We need to be accountable for our decisions and actions that we take

• Ensure you keep key correspondence

3

Label all your documents clearly

• Does the name of your document or folder actually tell you what's in it?

• Do all your titles and filenames follow your directorates naming conventions?

• Have you applied appropriate version controls to your document that give others a clear picture of its status?

• Would another member of staff know what the folder or document was, just by looking at the title?

4

Dispose of information securely and get rid of anything trivial or redundant

Be sure what you keep has a business purpose.

• Do you regularly review your documents to see if they're still necessary to keep?

• Do you know how to dispose of information securely?

• Are you aware of the retention periods on your documents?

• Is the information you're storing out of date or inaccurate?

### What's in a name?

We ask you to follow our naming conventions because it makes it easier for you and everyone else to search for, retrieve and understand the information we have.

Bad practice

Can you tell what these documents are about without opening them up? We don't think so. Now imagine having to do this every time – time-consuming, right?

When the documents were opened, they turned out to be:

• Management reports that were needed for inclusion in the annual report,

• Minutes of a meeting with a key external stakeholder, and

• Detailed notes about the decision to take enforcement action against a bank

Good practice

Now that's better. The titles used in these examples are descriptive and consistent. It's clear who the information is from and what it contains.

Here are some general principles to follow:

• Keep filenames short, clear and meaningful

• Use a consistent and logical approach – order the name of a file in a way that makes it easiest to retrieve, for example by date or project name

### Version and document control

Version and document control is good practice in Information Management.

Version history

Using clear and meaningful version numbers is just as important as using the right filename. We all need to track changes that have been made to our documents and make sure we're referring to the latest version. Use major versions for the final document. Eg 1.0 or 2.0

Use a minor versions for drafts eg 0.1

If a document's named 'final' yet there's another document with the same name created on a later date, how can we be sure which is the right document to look at?

Document control

The status and history of important documents should be clear. You should include a document control panel at the end of a document. For example, if you are writing a new HR policy or a piece of guidance, the document control panel will show who has contributed or edited the document and when it was agreed and published. This helps us to know how a document arrived at its final version and when it was applicable.

You can also use watermarks such as ‘draft’ or ‘confidential’ to show status. These are our basic requirements for version and document control. How it is achieved will depend which system you are working in. More information about version control is available in our version control policy.

### Can you spot good practice?

Have a look at these examples of saved records. Can you spot the ones that follow good practice?

1 Re: Delegates

\_shouldBeSelected false

2 20180306 ICO to MoJ DP Bill amendments (email)

3 ICO Information Management Policy v2.0

4 Image001.jpg

5 Correspondence 02/03/2018 [104600]

6 SLT Meeting minutes - 20180401 v1.0

\_feedback correct

That's right.

Our naming conventions apply to documents and emails and should be short, clear and meaningful. The key thing is to be consistent with your colleagues. Speak to your LIMO or Site Owner to find out if your department has a specific way of naming certain documents.

\_ feedback incorrect

That's not quite right.

Our naming conventions apply to documents and emails and should be short, clear and meaningful. The key thing is to be consistent with your colleagues. Speak to your LIMO or Site Owner to find out if your department has a specific way of naming certain documents.

### Save information on corporate systems so that we can access it

Think back to the scenario at the start of this topic. The information found wasn't in the right place.

Where should the information on the completed case be saved?

1 On the casework system

2 On an ICO laptop kept in a locker

3 On an ICO mobile device

4 Hard copies kept in a marked up storage cabinet with a note on the case to say where they were

5 In an ICO Outlook email account

6 On a personal drive

7 In Microsoft Teams

\_feedback correct

That's right.

We must ensure that we can access all of our corporate information. It needs to be managed and we need to provide access to it if it is requested. Electronic information needs to be kept on the right corporate system. Remember to move your information from Microsoft Teams to our casework systems or SharePoint EDRM as soon as possible. Hard copies can be kept in a locked or passcode protected storage cabinet or secure team storage, but not in a personal locker. If it's not easy for other people to access it, it can't be managed or used.

\_ feedback incorrect

That's not quite right.

We must ensure that we can access all of our corporate information. It needs to be managed and we need to provide access to it if it is requested. Electronic information needs to be kept on the right corporate system. Remember to move your information from Microsoft Teams to our casework systems or SharePoint EDRM as soon as possible. Hard copies can be kept in a locked or passcode protected storage cabinet or secure team storage, but not in a personal locker. If it's not easy for other people to access it, it can't be managed or used.

### Managing your inbox

We all know that our email inboxes get filled up pretty quickly. Imagine that a colleague's inbox is particularly full. Which of the following actions do you think they should not do?

1 Save case-related emails to the casework management system

2 Set aside some focused time each week to manage emails

3 Save meeting minutes to the relevant casework system or shared folder in SharePoint EDRM

4 Keep copies of complaints and decisions on your ICO laptop

5 Keep draft emails (even though final versions have been sent)

6 Save all emails to your drive until you've got time to review them

7 Keep re-sending emails to yourself to extend the retention period

8 Delete all emails to avoid managing them properly

\_feedback correct

That's right.

Inboxes are not a long term storage solution. Emails are automatically deleted after 12 months and we don’t have everyday access to everyone’s account. The best advice is to plan regular time to do your housekeeping. Imagine the challenges if you lost an email from your team member with a performance update that you wanted to refer back to later. Or you lost an email with evidence for a case.

Remember that once information has been deleted, you have lost access to it. Set aside time to do your housekeeping - making sure important corporate information is saved into the right system, with the rest properly deleted.

\_ feedback incorrect

That's not quite right.

Inboxes are not a long term storage solution. Emails are automatically deleted after 12 months and we don’t have everyday access to everyone’s account. The best advice is to plan regular time to do your housekeeping. Imagine the challenges if you lost an email from your team member with a performance update that you wanted to refer back to later. Or you lost an email with evidence for a case.

Remember that once information has been deleted, you have lost access to it. Set aside time to do your housekeeping - making sure important corporate information is saved into the right system, with the rest properly deleted.

### Do we still need it?

It's crucial that we keep important information, but at the same time we need to effectively manage redundant, outdated or trivial information. Through regular housekeeping activities you should review, weed and delete information that is no longer of value. For example draft versions of a document you have since completed.

It's important that we can show that our information is accurate and up to date and we're not keeping it longer than we need it. We have a Retention and Disposal Schedule to help you to make sure information is managed and securely disposed of without delay.

This is especially important for personal data, including your own personnel file. We must regularly review records containing personal information so that if we no longer need it, we can delete it.

### Retention periods

Our Retention and Disposal Schedule defines the retention periods of our records.

Can you match the record with its retention period?

placeholder Please select an option

1 An employee expenses claim

12 months

4 years

6 years

2 Sick leave

12 months

4 years

6 years

3 An appeal to the Information Tribunal

12 months

4 years

6 years

4 An email in an inbox

12 months

4 years

6 years

\_feedback correct

That's right.

Emails are automatically deleted from Outlook after 12 months. Records of Tribunal appeals and expenses claims are reviewed 6 years after closure and details of sick leave is usually kept for 4 years. Some information might need to be kept longer. For example, your pension information will be kept until you're 100 years old.

\_ feedback incorrect

That's not quite right.

Emails are automatically deleted from Outlook after 12 months. Records of Tribunal appeals and expenses claims are reviewed 6 years after closure and details of sick leave is usually kept for 4 years. Some information might need to be kept longer. For example, your pension information will be kept until you're 100 years old.

### Secure disposal

The right method of disposal is key - let's look at an example.

What are suitable methods of disposal of paper work?

1 Confidential shredding bin

2 Wastepaper bin

3 Cross-shredder

4 Recycling box

\_feedback correct

That's right.

Once something is no longer needed, you should use confidential shredding bins or cross-shredders. Never put papers into general waste, recycling bins, public bins or your bins at home. Ask if you’re not sure whether something is still needed and if required, update the record to show that it has been disposed of.

\_ feedback incorrect

That's not quite right.

Once something is no longer needed, you should use confidential shredding bins or cross-shredders. Never put papers into general waste, recycling bins, public bins or your bins at home. Ask if you’re not sure whether something is still needed and if required, update the record to show that it has been disposed of.

### Data protection by design and default

We must consider data protection and privacy issues in everything that we do and it pays to think about it at the very beginning. We can’t be sure that we are doing what we should be if it isn’t. By default we should commit to processing the minimum amount of personal data necessary to achieve our purpose. Here are some examples.

1 "We bought and implemented a new electronic system for processing all our staff information, including sensitive information.

We’d been using it successfully for about six months when we were asked to delete some ex-employee data. It was only then we realised that the system didn’t have a delete function.

And because we weren’t able to comply with our legal obligations around deletion, we could no longer use the system. All the effort and money was wasted."

2 A Data Protection Impact Assessment (DPIA) at the beginning would have prompted the team to consider all the legal and governance requirements and would have identified the issue of deletion as part of the process. If the supplier was unable to offer any deletion options, we’d have used a different supplier. The outcome of the DPIA might be that we can't go ahead with our plans.

3 Everything we do should have privacy built into its design.

We need to assess impact on privacy and security of what we are thinking of doing, even if it seems like a small change or is something that we need to do like get more office space or update our processes. Impact assessments help us shape the design of the outcome and build in proportionate solutions to reduce the risks.

Design, risks and solutions should be documented along with updates as work progresses.

4 A DPIA or similar assessment will help you to identify if you need to:

• Update privacy information we provide to customers or staff

• Update our records of processing activities

• Add new security controls

• Update our retention and disposal schedule

• Complete a supplier audit or questionnaire

• Update our contracts register

• Update our information asset register(s)

• Ensure our records of consent are accurate and up to date

• Update our appropriate policy documents

• Ensure appropriate protection for data transferred internationally

You can find some detailed guidance on how to complete a DPIA at the ICO on ICON.

### Data Protection by design and default

In which of the following situations should you think about carrying out a DPIA?

1 When considering using more CCTV cameras at our offices

2 When thinking about new ways we might get intelligence to help our investigations

3 When contracting with a new provider of occupational health services for our staff

4 When introducing an IT upgrade with new functionality that we haven’t used before

5 When putting on an event for stakeholders at a different venue

\_feedback correct

That's right.

You should consider carrying out a DPIA for all the examples. You can see that most processes have a potential impact on privacy and security.

• When using privacy intrusive techniques such as CCTV – is it a proportionate solution to the risk or problem?

• When introducing new IT functionality – it might look exciting but is something going on in the background which is doing new things with our data? Do we want it to do that?

• When considering any new supplier, being particularly careful when we will be giving them sensitive information, such as your health data.

• When thinking about new ways to collect data – even if the aim is to help our investigations.

• When hosting an event – are you taking photos or filming? Do you need to record dietary requirements for food? Does the venue have WIFI or lots of CCTV?

\_ feedback incorrect

That's not quite right.

You should consider carrying out a DPIA for all the examples. You can see that most processes have a potential impact on privacy and security.

• When using privacy intrusive techniques such as CCTV – is it a proportionate solution to the risk or problem?

• When introducing new IT functionality – it might look exciting but is something going on in the background which is doing new things with our data? Do we want it to do that?

• When considering any new supplier, being particularly careful when we will be giving them sensitive information, such as your health data.

• When thinking about new ways to collect data – even if the aim is to help our investigations.

• When hosting an event – are you taking photos or filming? Do you need to record dietary requirements for food? Does the venue have WIFI or lots of CCTV?

### What should a DPIA cover?

Display Title What should a DPIA cover?

Your DPIA must:

• Describe the nature, scope, context and purposes of the processing. It should be clear about what personal data is being processed and for what reason.

• Assess necessity, proportionality and compliance measures.

• Identify all relevant risks to the rights and freedoms of individuals, assess their likelihood and severity and detail measures to mitigate these risks.

### Relationships with other organisations

If your business area is working with or sharing information with another organisation, the relationship needs to be defined and documented.

1 What is the relationship?

You need to determine the nature of the relationship you are setting up. Are you asking them to provide a service for us? Are you asking them to process personal data for us?

2 Will we need to provide them with personal data?

If you are sharing personal data, you need to be very clear about what you are asking or allowing them to do with it.

3 Work with Commercial Legal

Inform Commercial Legal about any agreement or contract you want to enter into.

4 Document the relationship

This could be a formal contract, a confidentiality agreement, or a memorandum of understanding. Whatever form it takes, it will need to be clear about what we are asking them to do, how and why.

### Our most valuable asset

Through good information management we can help get the right information to the right people, and keep it no longer than we need it. This helps us avoid reputational risk, save time and guarantee trustworthy and reliable information.

Keeping good records of the work we've done and the decisions we've made shows our accountability, and demonstrates to others how we are meeting our legal obligations.

Remember to:

• Think privacy at the beginning! What is the privacy and security impact of what you want to do?

• Label all your documents clearly

• Save information in the right place so others can find it

• Dispose of information securely when the retention period expires

• Get rid of redundant, outdated or trivial information

• Familiarise yourself with our corporate standards and any local information management practices in your department.

## Page – 3 - Transparency

15 mins

### Open and transparent

Transparency is vital to ensure we have the trust of our customers, stakeholders and staff.

We provide privacy information on our website and in our offices for everyone who comes into contact with us. This information tells them what we do with their personal data. We keep this accurate and up to date by reviewing it on a regular basis. We also promote transparency by responding to information requests and proactively publishing as much information about our work as we can.

### Transparency and trust

We publish privacy information and make it available as early as possible whenever anyone contacts us or we contact them. We need to ensure that we do what we say we will.

To keep this up to date, we need to have a clear view of how we process personal information.

This helps keep the trust of customers, stakeholders and staff.

1

There are several mechanisms to help us keep track of the personal data we are processing:

• Information asset registers

• Contracts register

• Record of processing activities document

• Data Protection Impact Assessments

• Retention schedule

• Process and policy documents

• Appropriate policy documents explaining our processing of special category data and processing for law enforcement purposes

• Records of decisions to share

• Records of decisions to transfer abroad

2

If you are involved in any business projects or service updates, you must make sure that policies, procedures and other personal data registers and documents are kept up to date.

This will help you know what personal information we have, where it is and what we are doing with it. We need to know this to be able to keep our privacy information up to date.

### Do not obstruct transparency

It could be a criminal offence if you do. The offence relates to trying to prevent disclosure of information that has been requested under freedom of information or data protection laws.

1 What not to do

When a request is received, any information relevant to the request that we hold at that time, must not be:

• Altered

• Defaced

• Blocked

• Erased

• Destroyed

• Or concealed

You could be personally liable if you do.

2 Producing all relevant information

We receive many requests for information and you will find that you are often asked to produce any information you hold or know of. All of the good information management techniques we talked about in the Accountability section will make this easier for you to do. When this happens, please ensure that you send all information you think might be relevant to the request. It might not end up being disclosed to the requester, but it needs to be considered.

### Telling people what we do with their data

We are open and transparent about the way that we process personal data and about the work that we do.

1 We provide detailed privacy information to our customers and stakeholders about all our processing of personal information in our privacy notice.

We provide detailed privacy information to our customers and stakeholders about all our processing of personal information in our privacy notice, for example it explains our processing in relation to:

• Our recruitment processes

• Our complaints and investigations processes

• People who attend our events

We provide detailed privacy information for ICO staff in our Staff Privacy Notice. This covers things like:

• Our employment contracts

• Our health and wellbeing

We publish information about our work, for example,

• Expenses information of our senior leadership team

• Corporate strategies and priorities

• Regulatory action we take

Check our website for updates – it can be an easy answer to a question from a customer.

2 We disclose information in response to specific requests made under the data protection laws, Freedom of Information Act or Environmental Information Regulations.

We disclose information in response to specific requests made under the data protection laws, Freedom of Information Act or Environmental Information Regulations.

Examples of information we might disclose include:

• An individual's own personal data

• Documents from a case file where disclosure won’t prejudice our work

• Our expenditure and contracts

There may be times, though, when we're not able to disclose information for good reason and because it is exempt.

If you're not sure whether to disclose information or not then just ask your Manager or the Information Access team.

3 Remember that all information we hold and information you create on behalf of the ICO could be disclosed.

Remember that all information we hold and information you create on behalf of the ICO could be disclosed.

This might include:

• Draft documents

• Meeting notes on your ICO device that you made quickly and meant to delete

• The email you sent to your manager about a frustrating complaint

• And the letter you sent to a stakeholder explaining you don't think their new idea is a good idea

Embarrassment is not an exemption so we need to be professional and state our position clearly.

### Why might we be asked to disclose information?

Who might ask us for information?

When we have to share personal data with a third party consideration should always be given to data minimisation.

1 A colleague asking for their personal data

2 A police officer as part of an ongoing police investigation

3 A complainant or organisation asking for documents from their case

4 A public inquiry or court order

5 Any individual/organisation under freedom of information/environmental information regulations

\_feedback correct

That's right.

All of these people or groups request information from us. We need to make and record a decision on whether we can lawfully disclose information to them.

\_ feedback incorrect

That's not quite right.

Actually, all of these people or groups request information from us. We need to make and record a decision on whether we can lawfully disclose information to them.

### Our data protection rights

Data protection gives us all specific rights to ask about what is being done with our personal data. Some rights are only applicable in limited circumstances. You need to be aware of the rights and able to recognise them – many of them have a short timescale for us to respond. If you’re not sure if it’s a request, ask a manager or contact accessicoinformation@ico.org.uk.

1 Right to access their own information

If we hold personal information about an individual, they are entitled to ask us for copies and we have one calendar month to reply.

2 Right to be informed about what we're doing with their personal data

If someone asks "What do you do with my data?", direct them to our Privacy Notice on the website. Alternatively, send them a copy or read it to them. Remember requests can be made verbally and in writing.

3 Right to have personal data erased

This is known as the 'right to be forgotten'. If someone asks us to do this and we have no legitimate reason to continue to process the data we would need to erase it. We have one calendar month to reply.

4 Right to have data corrected if it's inaccurate or completed if it's incomplete (rectification)

A customer might ask you to update their contact details, or add a note to say they disagree with the outcome of the case. We have one calendar month to reply.

5 Right to object to the processing of personal data

If someone doesn't think we should be processing their personal data or thinks we no longer need to, they can ask us to stop. If it's marketing we must stop immediately. We have one calendar month to reply.

6 Right to data portability

This allows individuals to move, copy or transfer personal data easily from one IT environment to another. This is unlikely to apply often at the ICO. We have one calendar month to reply.

7 Right not to be subject to a decision based solely on automated processing

This relates to processing where there is no human input and which has a significant effect on individuals, and we have to inform individuals if they are subject to it. We need to assess the impact to individuals before doing any automated decision making. We have one calendar month to reply.

8 Right to request restriction or suppression of their personal data

This relates to the restriction of data and limiting its use, especially where the accuracy or use of the information is contested, or they object to the processing. We have one calendar month to reply.

### Right to official information

Freedom of Information and the Environmental Information Regulations give individuals the right to ask for official information. We have 20 working days to respond - below are some examples of information we might disclose.

1. Information about how many staff we have and which suppliers we use.

Disclose

Don't disclose

2 Your manager has given you her personal mobile number for work emergencies while she's on holiday. A customer rings demanding to speak to her.

Disclose

Don't disclose

3 Information about our carbon footprint

Disclose

Don't disclose

4 Details about an ongoing investigation.

Disclose

Don't disclose

\_feedback correct

That's right.

It is important that we are open and transparent about our impact on the environment, resources, our suppliers and finances.

You should not disclose private information of colleagues. The customer will have to speak to someone else or wait for her return. Disclosing details of ongoing investigations is likely to prejudice our work and shouldn’t be done without consultation.

\_ feedback incorrect

That's not quite right.

As a public authority funded by the government and organisations we are accountable for the way we spend our money and allocate resources. We need a safe space to conduct our investigations and plan next steps.

### Spotting a request

Now look at what happened in the following scenario and answer the question that follows.

1 While a colleague was on a two-week well-earned holiday, they received an email with a request for copies of advice their team had recently provided to a stakeholder - a freedom of information request. They were so busy on their last day, they didn’t put their out of office message on.

When they got back to the office, they found they had almost 200 emails in their inbox, many of which were chasers because people thought they were ignoring them.

2 They dealt with the most urgent emails first and then the ones that needed some obvious action.

They totally missed the email with the request – it was without a subject heading and not from someone they dealt with regularly.

3 By the time they opened the email and realised it was a request for information, four weeks had gone by.

This meant the response was going to be late. A late response can result in a complaint and is a breach of the law.

### What went wrong?

What do you think led to this situation?

1 They should have checked their emails while they were on holiday

2 They didn't put their out-of-office message including the address to make requests to – accessicoinformation@ico.org.uk

3 It was the sender's fault for not being clear what the email was about

4 The response to the request was late in breach of FOI requirements, because they didn’t read their emails properly on their return to work

\_feedback correct

That's right.

If your colleague had read their email properly on their return to work, or at least put their out-of-office message on, the sender would have known to direct their request to someone else. There are strict timescales for responding to requests for information and this starts when the request is received by the ICO, and not when it's read. We have 20 working days to respond to a FOI request and one calendar month for requests about personal information made under data protection legislation.

\_ feedback incorrect

That's not quite right.

If your colleague had read their email properly on their return to work, or at least put their out-of-office message on, the sender would have known to direct their request to someone else. There are strict timescales for responding to requests for information and this starts when the request is received by the ICO, and not when it's read. We have 20 working days to respond to a FOI request and one calendar month for requests about personal information made under data protection legislation.

### Verbal requests - under data laws and the EIR

Having just got over the incident, the same colleague gets a call from a customer who emailed them at the start of their leave who thought they were being ignored. The customer asks for all of their personal data held by the ICO.

What should your colleague do?

1 Insist they put the request in an email first

2 Fill out a verbal request form and send it to the Information Access Team as soon as possible

3 Point the caller to our website as the information is already available

4 Pass the call to a manager or the IA team

5 Make a note of the call and put it to the bottom of the pile

\_feedback correct

That's right.

Requests for information can be made verbally. You can suggest they put the request in writing if it would be helpful – but you can’t insist. In most cases you should fill out the relevant verbal request form and send it to accessicoinformation@ico.org.uk. Don’t pass the caller around different colleagues - it should be easy and straightforward for someone to exercise their rights over the phone.

\_ feedback incorrect

That's not quite right.

Requests for information can be made verbally. You can suggest they put the request in writing if it would be helpful – but you can’t insist. In most cases you would fill out the relevant verbal request form and send it to accessicoinformation@ico.org.uk. Don’t pass the caller around different colleagues - it should be easy and straightforward for someone to exercise their rights over the phone.

### Can I just answer the question?

Some requests can be dealt with by the person or team who receives it rather than being passed onwards. If you can deal with a request yourself, you should.

Which of the following requests do you think you could deal with yourself and do not need to send to the Information Access Team?

1 "I want you to delete all the information you hold on me."

2 ”I want all the documents from the latest case you issued a civil monetary penalty on.”

3 "I'd like a copy of your Dignity At Work policy."

4 "Send me the response you’ve had from the hospital – it’s about me and my complaint.”

5 "Tell me the name of your manager and give me a summary of my case."

6 "I've lost the letter you sent me last week; please send me another copy."

\_feedback correct That's right.

Often the person asking for information just wants an answer and it's quicker if you deal with it. Make sure you know what we publish on our website as we can quickly direct people to information that's already there. Remember though, even if you are dealing with the request yourself, you still have to do it as soon as possible as the 20-day timescale still applies.

\_ feedback incorrect

That's not quite right.

Often the person asking for information just wants an answer and it's quicker if you deal with it. Make sure you know what we publish on our website as we can quickly direct people to information that's already there. Remember though, even if you are dealing with the request yourself, you still have to do it as soon as possible as the 20-day timescale still applies.

### Recognising requests

Requests can be sent to any of us. We have to be sure we're complying with the law and meeting people's rights to their own data and official information.

Remember to:

· Read all the correspondence you receive and check for information requests – they might not all be obvious.

· Listen to customers on the phone – they may be making a verbal request for information.

· Consider whether you can deal with the request yourself – if you're not sure, ask.

· Don't delay – we have strict timescales to follow; going outside of these can lead to a breach of the law and complaints.

## Page – 4 - Information Security

15 mins

### Safe and secure

All our information must be held and processed securely, and this applies to both our electronic and hard copy information. We have a secure cyber environment that we keep up to date with the latest technology. We all need to take steps to help protect us from attempts to get through our defences.

We also need to keep our hard copy information secure within our own buildings but also when we're on the move.

Every scenario is different – if you are not sure what you should do, ask!

### What is information security?

Information security is about protection of information including personal data.

Its main focus is protecting the confidentiality, integrity and availability of information.

1 Confidentiality

Confidentiality is about protecting our information from unauthorised people or processes. The risk to our electronic or hard copy data includes laptop theft, paper theft, password theft, or sensitive emails being sent to the wrong people. It also includes not discussing confidential information in a public space.

2 Integrity

Integrity means protecting information from unauthorised changes, for example someone abusing privileges to delete or edit something.

3 Availability

Our information must be available to authorised users when it's needed. This means being able to access our systems and email. This means preventing service disruptions due to power outages, hardware failures, system attacks upgrades.

4 Our information

Confidentiality is key for us across all our business areas. Maintaining confidentiality is how we all contribute to keeping our information secure.

### Security controls

We use classification of information to identify a suitable level of security to protect that information and make sure it's only available to the people who need it.

1 Government Security Classification

The Government Security Classification identifies three levels of classification and affects the way we handle it:

• Official (including Official Sensitive)

• Secret (very little, very few staff involved)

• Top Secret (none)

We need to classify information we create and respect the classifications given by other organisations. Most of our information is Official with some being Official Sensitive, for example, criminal investigations or HR records.

Official documents do not need to be marked but Official Sensitive, Secret and Top Secret do.

2 Access controls

We try and keep as many resources as open access as possible. However, there is some information that must be limited to the people who really need to see it. An example of this is our HR system; because it's classified as Official Sensitive only a small group of people can access it.

If you don't have access to something that you need to do your job, then ask. Equally, if you no longer need access to a particular system or information then please ask for it to be removed.

Remember, that just because you have access doesn’t mean you have a legitimate need to view that information. For example, records of our criminal investigations.

3 Handling instructions

As well as using classifications it can be helpful to mark documents with handling instructions. These can be particularly useful when sharing information, for example by email. Providing clear handling instructions to those you share information with helps maintain confidentiality. Examples include:

• For HR use only – this information should only be shared with HR colleagues.

• Do not share further – the information is for your eyes only and should not be shared.

• Consult the originator before sharing – you may be able to share this information but you first need to check with the person who created it.

### Working on the move

Read the following scenario and answer the question that follows.

A colleague is going to work on the move for the next few days. They have a hectic schedule so decide to catch up on work while travelling.

Yesterday, they couldn't find the charger for their ICO device so decided to take their personal laptop with them. They had emailed the case file they were working on to their personal email address so that they could keep up with work, and gave their colleagues their personal email address so that they could keep in touch.

Which actions do you think has put ICO's information at risk?

1 They encouraged colleagues to email their personal address

2 They sent confidential information to their personal laptop

3 They have information held on a computer which is unlikely to meet our security standards

\_feedback correct

That's right.

Your colleague shouldn't have used their own equipment. We issue equipment for you to use and where allowed this can be used on the move, or at home. Information can be taken out of the office with appropriate authorisation - so make a record that you've taken it out.

\_ feedback incorrect

That's not quite right.

Actually, your colleague shouldn't have used their own equipment. We issue equipment for you to use and where allowed this can be used on the move, or at home. Information can be taken out of the office with appropriate authorisation - so make a record that you've taken it out.

### Working on the move or at home

The right preparation and knowledge will help to keep our information secure when you're travelling or working remotely. Here are some things to remember.

1 What you can do to protect information

• Familiarise yourself with the mobile device guidelines.

• Get permission from your manager before you take any ICO material outside the office and make sure you log it.

• Store any papers you have to take home in a locked unit which is not on display.

• Shred paperwork as quickly as possible when it is no longer needed. Use a cross cut shredder.

• We have rules about working from home. Make sure you follow our guidance and take the necessary steps.

• When instructed by IT, make sure you complete updates as quickly as possible.

• Always make sure media is encrypted before removing it from the office.

2 What you should avoid

• Don't discuss work matters on public networks or where you risk being overheard.

• Don't save any corporate information to a non ICO device.

• Don't leave mobile devices or papers unattended in public spaces.

• Don't take information out of the office without authorisation and log it.

• Don't attach your printer at home to your device. Be aware of the requirements you need to fulfil before you are authorised to print at home.

• If you’re working in a public place, be aware of your surroundings. How many times have you looked at the laptop of the person sitting next to you?

### In the office

Read the following scenario and answer the question that follows.

1

A colleague has a big meeting today with three external stakeholders and has a lot to prepare. They just sent their papers to print when reception tell them they have arrived early.

They pick up some hand-outs from their cluttered desk and goes to meet their visitors. Although they're rushing, they remember to lock their screen when leaving their desk.

2

They have met two of their visitors before, but doesn't know the third visitor. Reception is busy as lots of people are arriving at the same time. They are careful to check who their visitors are and make sure they have their named access passes from Reception before the visitors are taken to the meeting room.

Once in the meeting room, they remember they need the papers they sent to print. They have to leave their visitors for a few minutes to get them.

3 When they return to the meeting room, they find that one of the visitors has left the room. When they give out copies of the hand-outs, they discover some sensitive papers tucked in with them. They had picked them up from their desk by mistake.

### What went wrong?

Which do you think are examples of bad practice?

1 Papers were left on the printer

2 Visitor name badges were checked

3 Visitors were left unattended

4 They locked their screen

5 They didn't check the handouts they had with them

\_feedback correct

That's right.

Your colleague did the right thing by checking the name badges of their visitors, and locking their screen before they got up.

However, it's bad practice to leave visitors unattended. Your colleague should have been more thorough in checking their handouts, and been alert to anything they might have left by the printer

\_ feedback incorrect

That's not quite right.

Your colleague did the right thing by checking the name badges of their visitors, and locking their screen before they got up.

However, it's bad practice to leave visitors unattended. Your colleague should have been more thorough in checking their handouts, and been alert to anything they might have left by the printer

### How can you help?

Think about what you can do to protect information in your role.

Remember, if something goes wrong or nearly goes wrong, no matter how it happened, report it as a security incident.

• Don't allow anybody to follow you through secure doors, and straight away report anyone who doesn’t have an ID badge

• Escort your visitors – make sure reception know they are coming

• Dispose of information or hardware securely

• Remember that not everyone has access to the same information

• Before sharing confidential information, check its security classification, and check that the requester had a business need to see it and you have the authority to send it. If you're not sure, ask

• Lock your screen when you leave your desk

• Wear your ID badge at all times and if you lose or mislay it, report it immediately

• Always use e-redact when redacting information

• Encrypt all removable media before they leave the office

• Check and double check recipient addresses.

### At the desk

Read the following scenario and answer the question that follows.

1

A colleague's bus is stuck in traffic and they're running late for a meeting. They call a member of their team to get their laptop up and running to save them a bit of time when they finally get to the office.

The team member asks for their password.

"It's JANalex55, ah, no, that was last month's; I think it's FEBalex56 now… Actually, I really can't really remember; could you check it against the list in my notebook? It's on my desk."

2

While the team member waits for their colleague to get into the office, an email catches their eye.

From: Alex@ico.org.uk

Subject: Urgent action required

You must download the following attachment on your device as soon as possible to help secure our systems.

Sec.exe

3

The team member is suspicious as the address doesn't look right, but forwards it to the managers in their area to see if anyone knows what it is.

### What did they both do wrong and what should they have done?

Which actions do you think have put the ICO's information at risk?

1 They shared their password with a colleague

2 Their password is easy to guess

3 The team member forwarded the email even though they thought it looked suspicious

4 They should have contacted IThelp immediately

5 They kept a list of their passwords in a notebook by their computer

\_feedback correct That's right.

You shouldn't share your password with anyone. It's also too simple and not stored securely. You shouldn't forward the suspicious email, even if you were intending to contact IThelp afterwards.

\_ feedback incorrect

That's not quite right.

You shouldn't share your password with anyone. It's also too simple and not stored securely. You shouldn't forward the suspicious email, even if you were intending to contact IThelp afterwards.

### Passwords

Think about what you can do to keep our information secure. And if something does go wrong, report it immediately.

How to keep your passwords safe

You should never share your password. If you have to write them down then store them somewhere safe, out of sight, and (most importantly) away from your device. Make sure you keep personal and work passwords completely separate, so a personal one can’t be used to guess a work one.

What to consider when creating a password

• Choose a password that is difficult to guess but easy for you to remember - something that's personal to you and only you would know. In general, the longer the password is the harder it is to crack.

• Don't recycle passwords (remember the example above)

• Try turning a sentence into a password, eg "My first house was 120 Fake Road" becomes "mfhw120fr". Alternatively, create a passphrase by using three or more random words, eg "correct horse battery staple".

• Avoid using the same password for multiple accounts. If one is compromised all are compromised.

• Use a combination of characters - avoid (single dictionary or misspelt) words, but do use upper and lowercase, numbers and punctuation.

### Suspicious emails

There are a lot of attempts to send us emails that contain viruses or links to other malicious sites which could infect our systems or extract our data. Most of them get stopped before they get through our perimeter. However, we do receive some suspicious emails, and we need you to be alert to them. Some are very convincing and targeted.

How to spot a suspicious email

Common characteristics of malicious emails are:

• Unexpected email

• You don’t recognise the sender

• Has a generic subject line such as ‘Invoice’

• Addresses you as 'Dear customer'. Most legitimate contacts will know your name

• Contains links in the body of the email

• Tries to make you act quickly by suggesting an urgent response is needed.

Remember, if the email feels suspicious, unexpected or unusual you should report it.

What to do if you spot a suspicious email

If you have received an email you think is suspicious:

• Don’t open it

• Don’t click on the links or open attachments

• Don’t forward it on to colleagues or externally

• Report it immediately using the “Report Message” button in your Outlook toolbar.

Remember, never use your ICO email address to sign up for anything that isn't work-related to reduce potential email attacks.

### Spot the risks

There are lots of security risks in and around the office that we can all avoid. Look around you. Can you see anything that looks like this?

\_graphic alt Series of pictures including; paperwork, USB flash drive, waste paper bin, email inbox, redacted email, mobile device

1 Paperwork

Always assess your surroundings and never leave confidential documents unattended. If you find something that looks confidential, you must take personal responsibility for handing it in to your manager or Information security.

2 USB flash drive

The loss or theft of removable media can result in a serious data breach if confidential data falls into the wrong hands. All media transfers must be approved by the Cyber Security Service to ensure the data is appropriately protected in transit.

3 Waste paper bin

Don't put paper into waste bins even if it's not sensitive. Get into the habit of using shredding bins or cross shredders. Even newspapers – all paper gets shredded and recycled.

4 Email inbox

It's easy to overlook an email sent with the wrong attachment, sent to the wrong address, or with a long email chain, but this could mean someone's details or sensitive information is sent to the wrong person. Imagine HR sending information about your sickness absence to someone with the same first name. Aim to minimise what goes out – if you don’t need the whole email chain, cut if off.

Always check the email address before you send your email and disable auto-fill in Outlook.

Be careful if you're sending email to multiple people using a group list or the 'reply to all' feature. Ask yourself: Does everyone really need to see this information?

5 Redacted email

Some information may need to be redacted before it can be shared.

To remove the sensitive information from a document we must use e-redact software.

6 Mobile device

Always keep your mobile devices close by. Never leave them unattended. Don't leave any mobile device in your car, on public transport, in hotels or meeting rooms. Imagine leaving your work tablet on the back seat of your car and the car gets stolen.

Don’t leave mail in our mail hubs overnight – lock it away.

### Report quickly!

Don't be afraid to report security issues, including near misses - even if you think you're the one who's made the mistake. It may not turn out to be an incident, but we learn a lot from near misses. The incident will be much harder to manage if you delay – or worse – don't say anything at all!

Report all suspected incidents by completing the 'Security Incident Report Form' which is available on ICON and send it to info.sec@ico.org.uk immediately.

If you lose something like a mobile device or ID badge, even if you think the loss is only temporary, report it. Lost devices should be reported to 0330 414 6886 which is manned 24/7, and lost ID badges should be reported to Facilities immediately.

Don't delay reporting the loss because the potential consequences for ICO and you personally can quickly escalate. All suspected incidents have to be reported to Information Security immediately or within 24 hours to ensure we comply with our UK GDPR breach reporting obligations.

### How to avoid inappropriate disclosures

1 A colleague was really busy working on cases. One of their new customers was called Andrew Jones. When they did their check to see if Andrew Jones was an existing customer, they found an existing customer record but forgot to check the address details.

They selected to use the existing customer record.

2 This was not the same customer and they ended up sending a letter detailing their new customer’s sensitive complaint to the existing customer.

They were alerted to what they’d done by the existing customer. At this point, they had to tell their manager, who in turn had to inform Information Security.

3 The new customer, Andrew Jones, made a complaint about the disclosure of his personal information. The existing customer, Andrew Jones, also complained because he didn’t think we were taking our customers’ privacy seriously, even though it wasn’t his data we disclosed.

4 The team manager and our Information Security team spent several hours investigating the incident, what went wrong and how to stop it happening again. The manager also had to write to both customers to apologise.

Your colleague had to spend a lot of time explaining what they’d done and why they hadn’t made the necessary checks. Their team manager also explained that the incident would be recorded in his annual performance review which was coming up and they would discuss it further then.

5 To avoid making the same mistake, always make sure you're thorough in your approach:

• Double check recipient names and addresses

• Double check your content/attachments

• If you need to redact information, use our e-redact software

• Make sure you’re speaking to the right person if discussing personal or confidential information over the phone

• If disclosing Excel sheets – do not hide columns; delete them instead. Save in csv format where possible

• Disable auto-fill in Outlook

• Avoid typing out email addresses - select from an existing list or copy and paste.

### What might go wrong?

Which of these do you think pose an information security risk?

1 Sharing a password

2 Leaving a bundle of papers on a train

3 Sending an unencrypted disc or USB

4 Not keeping your devices updated

5 Not checking recipients' contact details

6 Not recognising suspicious emails

\_feedback correct

That's right.

All of these things are easy to do and have happened. Some are riskier than others, but avoiding all of them helps to ensure our security and confidentiality. You and your colleagues are our first and strongest line of defence against risks to our information and property. By following a few simple security measures, you can help us prevent these security incidents.

\_ feedback incorrect

That's not quite right.

Actually, they could all happen. Some are riskier than others, but avoiding all of them helps ensure our security and confidentiality. You and your colleagues are our first and strongest line of defence against risks to our information and property. By following a few simple security behaviours, you can help us prevent these security incidents.

### Things to remember

Knowing how to securely handle information is important. A breach of security can lead to serious consequences for everyone, so understanding how information can be vulnerable in your job role is crucial.

Our Security Manual contains tips and advice to help develop good security practices at work and can be used to identify and avoid mistakes.

At all times:

• Think about what you are doing

• Don't be rushed or take shortcuts

• Check before you share or disclose anything

• Report any suspected or actual security incidents to info.sec@ico.org.uk immediately

• If you're unsure, please ask your manager or Cyber security.

## Page – 5 - Final Assessment

### Final Assessment

You'll now be asked ten questions based on the main learning points of this module.

You need 90% to pass the assessment.

If you score below this, you'll be prompted to return to the module to review the topics. When you feel ready, you can try the assessment again.

Select all that apply for each question, then click or tap Submit at the bottom of the page.

### Q1. How do we make sure our customers, stakeholders and staff have trust and confidence that we are accountable and transparent about the way we handle their information?

1 We let all of our staff have access to all of our information

2 We publish privacy information for everyone in contact with us

3 We know what information we have, why we have it, where it is, whether we need it and what we’re doing with it

4 We make sure we record our information in a way that we can find it, understand it and provide access to it

### Q2. Who is responsible for properly managing ICO information? Select all that apply

1 Facilities and Information management Teams

2 The DPO

3 All staff

4 Information Asset Owners

### Q3. We receive requests from individuals who are exercising their rights under data protection and freedom of information law. Which of the following are true?

1 The deadline clock for response starts as soon as the request is received by the ICO

2 The deadline clock for response starts when you have read the request and decided it is a request. If you don’t read it, we don’t have to respond

3 Any relevant information held at the time of the request might be disclosed even if it is embarrassing

4 After a request has been received, if I delete or alter information with the intention of preventing it being disclosed, this is a criminal offence

### Q4. I’m working on a project to deliver a new service. We’ll be using new technology and working with a third party. I need to…

1 Build in time through the life of the project to assess the privacy and security risks

2 Work out solutions to the risks and make sure they are implemented before the service goes live

3 Make sure we have a contract with third party and be clear about what we are asking them to do

4 Plough on! There’s a deadline for my project and I don’t have time to talk about data protection

### Q5. Other people need to be able to understand the work you have done. Your work might be scrutinised. For what purposes might we need to produce our records?

1 Select Committees or parliamentary questions

2 FOI requests or Tribunal cases

3 Public inquiries

4 Court orders or requests from other regulators

### Q6. We've made a decision to disclose some information. How do you make sure you don't disclose the information that isn't suitable for disclosure?

1 Use a black marker pen!

2 Use our redaction software – e-redact – to redact the information that isn’t suitable for disclosure

3 Don’t disclose any information

4 Check for hidden cells, personal data or tables in a spreadsheet

### Q7. What steps can you take to avoid or manage inappropriate disclosures?

1 Always double check the name and address you are sending to. Double check your content!

2 Label your documents so you know what’s what

3 Check you are sending the correct annexes and attachments

4 Report any inappropriate disclosures to info.sec@ico.org.uk immediately!

### Q8. How should you store corporate information?

1 Keep it secure in your personal locker

2 Choose the appropriate corporate system, depending on what the information is

3 By regularly filing information in the right place

4 Use naming conventions and version control so we can find it and understand what it is

### Q9. What should you do before taking information out of the office?

1 Consider whether you need to take it in the first place

2 Just take it, there isn’t anything that you need to do

3 Read, understand and follow corporate guidance on taking, printing and storing information away from the office

4 Log it on your local team log

### Q10. Confidentiality is vital to us keeping the trust of our stakeholders and customers. How could it affect you?

1 A breach could result in disciplinary action

2 You should think before you speak about work with family or friends

3 You will always need to be careful. It applies during and after your employment

4 If you use ICO information recklessly or for your own gain - you could get a criminal record

### Assessment results

Score 0-89 feedback

Unfortunately you haven't achieved 90% in this assessment.

You may want to return to the main menu and revisit the topics, then try the assessment again.

Score 90-100

Well done. You have passed the assessment.