A guide to the legislation the ICO regulates

Upholding information rights for all

ico.

Information Commissioner's Office

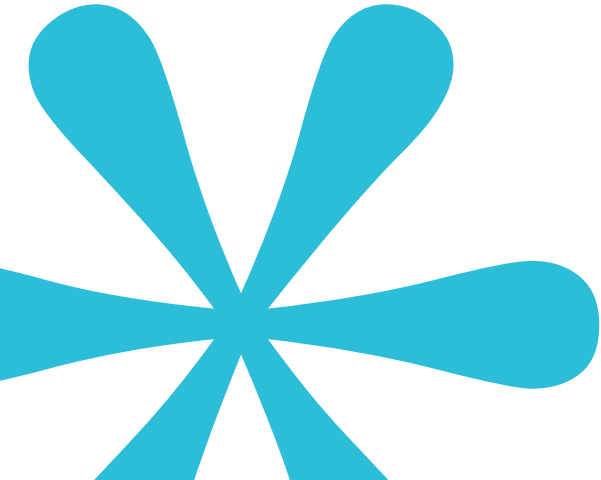
Contents

About the ICO

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK's independent public authority set up to uphold information rights. We do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.

The ICO enforces and oversees the Freedom of Information Act, the Environmental Information Regulations, the Data Protection Act and the Privacy and Electronic Communications Regulations.



The Freedom of Information Act 2000 gives people a general right of access to information held by public authorities. We aim to make public sector bodies more open and accountable. We also help people to understand better how public authorities carry out their duties, why they make the decisions they do and how they spend public money.

The Environmental Information Regulations 2004 provide access to environmental information. The regulations potentially cover more organisations than the Freedom of Information Act, including some private sector bodies.

The Data Protection Act 1998 gives citizens important rights, including the right to know what information is held about them and the right to correct information that is wrong. The Act helps to protect the interests of individuals by obliging organisations to manage the information they hold in a proper way.

The Privacy and Electronic Communications Regulations 2003 support the Data Protection Act by regulating the use of electronic communications for unsolicited marketing to individuals and organisations.

Summary of the legislation

1. Freedom of Information Act 2000

Overview of the Act

This Act came fully into force on 1 January 2005. It deals with access to official information, while parallel regulations provide access to environmental information (page 14).

Any individual or organisation can make a request in writing for information held by a public authority.

The public authority should tell the applicant within 20 working days if it holds the information and, if so, provide it unless exemptions apply. If an applicant has asked for the information to be provided in a certain format, the authority should do so, if this is practical.

Public authorities must actively provide certain types of information by adopting and using the ICO model publication scheme. The scheme makes sure organisations produce a guide to the information they provide, how they make it available and whether or not they charge for it.

The Act applies to all information, including information that existed before the Act came into force.

Rights under the Act

The Act creates a right to know: the right of individuals to access information held by public sector bodies (public authorities).

A public authority can deny access in certain circumstances.

The public authority need not confirm or deny the existence of information or provide all or part of the information requested if:

- an exemption applies; or
- the request is vexatious (see glossary) or similar to a recent previous request; or
- the cost of compliance would exceed the 'appropriate limit' (see page 9).

If an exemption applies but it is 'qualified', this means that the public authority will have to consider whether the public interest in maintaining the exemption outweighs the public interest in releasing the information.

If the applicant is unhappy with the way their request has been handled, they should complain first to the authority in writing. The authority must then review the way they handled the request and the decisions they made.

If the applicant remains unhappy with the outcome of the review, they can complain to us, and we will investigate the case independently and decide on the appropriate course of action (see 'enforcement powers' on page 11). If the applicant or the public authority is unhappy with our decision, they can appeal to the First-Tier Tribunal, an independent body set up to hear cases about notices issued by us. The First-Tier Tribunal decision may not be the final decision as either party may take the issue further on a point of law.

Responsibilities of public authorities

Publication schemes
The Act places a duty on public authorities to adopt and maintain a publication scheme approved by the Information Commissioner.

We have developed and approved a model publication scheme that all public authorities should adopt.

The scheme:

- sets out the types of information a public authority must routinely publish;
- explains the way it must provide the information;
- states what charges a public authority can make for providing information; and
- commits the authority to providing and maintaining a guide to the information they provide, how they provide it and any charges.

Responding to requests for information
Public authorities have a duty to provide advice and assistance to help applicants who request information from them.

An applicant can express a preference for the information to be provided in copy form, as a summary or by inspection and which the authority should accept if practicable.

Public authorities should respond to requests for information within 20 working days.

If public authorities are withholding the information by applying an exemption for which they need to consider the public interest test, they may extend (by a reasonable period) their time for considering release of the information. The Commissioner recommends as good practice that this should be no more than a

further period of 20 working days. They must inform the applicant that they are doing this and give an estimated time for response.

Public authorities can refuse to provide information where it is estimated that the cost of processing the request exceeds the appropriate limit. The limit is £600 for government departments and £450 for all other authorities. However, authorities can recover the costs of communicating the information to the applicant, but this is limited to disbursements such as photocopying and postage.

If a public authority has grounds for not releasing the information requested on the basis of an exemption, it must issue a refusal notice. The notice must explain:

- what exemption it has applied and why;
- the public interest considerations it has taken into account (where applicable);
- the internal appeals process;
- the applicant's right to complain to us.

The exemptions

Public authorities need not disclose any information covered by one or more of the exemptions.

There are 23 exemptions in the Freedom of Information Act which are of two main types: those which are absolute and those which are qualified.

- **Absolute exemptions** – If one of these eight exemptions applies there is no right to the information under FOIA. Examples of an absolute exemption include personal information, information which is available by other means, and that which is barred from release because of another piece of legislation.
- **Qualified exemptions** – In all other cases, the exemption is a qualified exemption which means that the public interest in releasing the information must also be considered. The authority must therefore carry out a public interest test. Qualified exemptions cover a variety of subject areas ranging from national security through to commercial interests.

The public interest

The authority will have to decide whether the information should be released in the interests of the public. This public interest test involves considering the circumstances of each case in relation to the exemption that covers the information. The information must be released unless the public interest in maintaining the exemption outweighs the public interest in releasing it.

Exemption for personal information:

- If the information requested is about the applicant, the request must be addressed as

a 'subject access request' made under the Data Protection Act 1998.

- If the information requested is about a third party, a decision on release will be based on whether doing so would breach the Data Protection Act.

When applying any exemption a refusal notice must be issued providing an explanation of why the information is being withheld including which exemption/s have been applied, where appropriate the public interest considerations which have been taken into account, and the right to appeal the decision.

When refusing a request for information, an authority cannot withhold an entire document if only some of the information contained within it is exempt. An authority must provide a redacted (see glossary) version of the document along with a refusal notice stating why some of the information cannot be released.

The ICO's role and enforcement powers

The ICO continues to adopt a rounded approach to safeguarding information rights which reflects the different aspects of our role as educator and enforcer. This is done through:

- promoting good practice by public authorities in observing the Act;
- informing the public about the Act;
- approving a model publication scheme and ensuring compliance with it by monitoring the way the model publication scheme is adopted and operates;
- conducting assessments to check organisations are complying with the Act;
- issuing to public authorities notices such as:

  - information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
  - decision notices publicly detailing the outcome of the Information Commissioner's investigation into whether a public authority has complied with its duties under the Act in dealing with a specific request.
  - enforcement notices where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
  - practice recommendations specifying steps the public authority should take to ensure conformity to the section 45 and section 46 Codes of Practice;
  - undertakings committing an authority to a particular course of action in order to improve its compliance;
- prosecuting those who commit criminal offences under the Act; and
- reporting to Parliament on freedom of information issues of concern.

If the applicant or public authority disagrees with one of our formal notices, they may appeal within 28 days to the First-Tier Tribunal (Information Rights). A practice recommendation cannot be appealed.

If a decision or enforcement notice is served on a government department, the National Assembly for Wales, or any authority designated for these purposes by an order of the Lord Chancellor, it may be subject to an 'executive override', also known as a veto. In such a case a signed certificate from a Cabinet Minister, or equivalent, which is served and laid before Parliament within 20 working days, overrides the Information Commissioner's notice.

Freedom of information successes

The Freedom of Information Act is already making a significant difference to public life. Many people, including journalists, businesses, politicians, campaigners, and other members of the public have used the Act to request all kinds of information. The breadth of information made available to the public is shown by these examples:

- **Government**
  - Cost and use of official cars.
  - Compensation paid to IRA suspects.
  - EU subsidies paid to farmers.
- **Health and safety**
  - Surgeons' performance records.
  - NHS use of private hospitals.
  - Trials of new medicines.
  - Links between school dinners and Creutzfeldt-Jakob disease.
- **Transport**
  - Local authority income from parking fines.
  - Costs of transport projects, such as the second runway at Stansted Airport.
  - Number of fines issued by individual speed cameras.

2. Environmental Information Regulations 2004

The updated Environmental Information Regulations came into force on 1 January 2005. They implement European Directive 2003/4/EC on public access to environmental information.

Overview of the Environmental Information Regulations

Members of the public have the right to access environmental information held by public authorities.

Anyone can request environmental information, in writing, by telephone or in person.

The Environmental Information Regulations apply to most public authorities that are covered by the Freedom of Information Act. They also apply to any organisation or person carrying out a function of public administration, and any organisation or person under the control of a public authority who has responsibility towards the environment (including some private companies and public-private partnerships).

The definition of environmental information includes information on:

- the state of the elements of the environment, such as air, water, soil, land, landscape, natural sites and biological diversity;
- emissions, discharges, noise, energy, radiation, waste and other releases into the environment;
- measures and activities such as policies, plans and agreements affecting or likely to affect the state of the elements of the environment;

- reports and cost-benefit and economic analyses;
- the state of human health and safety, including contamination of the food chain; and
- cultural sites and built structures (as they may be affected by the state of the elements of the environment).

Regulation 12 provides public authorities with some grounds for refusing to disclose environmental information (exceptions).

All the exceptions are subject to a public interest test (see page 18). This means they must take into consideration the public interest factors in disclosing the information and those for withholding it and make a decision based upon the balance.

Public authorities must respond in writing within 20 working days.

An authority may charge a reasonable fee for providing the information.

As with the Freedom of Information Act, the Environmental Information Regulations can be backdated to cover all information, not just information recorded since they came into force.

Rights under the Environmental Information Regulations

The Environmental Information Regulations create a presumption in favour of openness. This means they presume that authorities will always aim to disclose information where they can, rather than withhold it.

Unless exceptions apply, the public authority should comply with the request for information, and where appropriate meet the requirements of Regulation 6 for the format the information is made available in.

If an applicant is unhappy with the way the public authority dealt with their request, they can complain to the public authority, which must then reconsider its decision.

If the applicant is still unhappy, they can complain to us, and we will investigate the case independently and decide on the appropriate course of action (see enforcement powers, page 19).

An applicant can appeal our decision to the First-Tier Tribunal.

Responsibilities for public authorities

Actively making information available

- Public authorities must make certain environmental information progressively available through electronic means, such as the internet.

- Public authorities must also organise their environmental information so that it can be systematically made public. Public authorities that are also subject to the Freedom of Information Act can use their guide to information as a way of complying in part with their responsibilities

to actively make available their environmental information to the public.

- There are minimum criteria as to what environmental information authorities are expected to progressively and systematically make available. These are stated in Article 7(2) of the European Directive (2003/4/EC).

- Public authorities who charge for information must publish these charges.

Responding to requests

The public authority must respond to the applicant within 20 working days, by providing the information requested or issuing a refusal notice. The time limit for response can be extended to 40 working days if a large volume of information is requested and the nature of the request is complex.

Public authorities must provide advice and assistance to applicants where necessary.

A public authority may charge a reasonable fee for environmental information. It cannot charge for environmental information held in public registers or lists or for viewing at the public authority's premises.

When refusing information the authority must provide an explanation of why the information is being withheld including which exceptions have been applied, the public interest considerations which have been taken into account, and the right to appeal the decision.

The public interest test

If an exception applies (see below), a public authority may choose to refuse the request and withhold the information. However, all the exceptions in Regulation 12 are subject to a public interest test. This means they must take into consideration the public interest factors in disclosing the information and those for withholding it and make a decision based upon the balance. There is a general presumption in favour of disclosure. This means the regulation presumes authorities will always aim to disclose information where they can, rather than withhold it.

Exceptions

An authority can refuse to provide information because:

- the authority does not hold the information or does not know what information is being requested;
- the request is 'manifestly unreasonable';
- the information is 'unfinished or in the course of being completed'.

Certain exceptions require the public authority to demonstrate the harm that would result if the information was released. Information can, for example, be withheld if release would adversely affect:

- defence, international relations, national security, and public safety;
- the course of justice, or the confidentiality of proceedings;
- intellectual property rights (trade marks, copyright etc);

- the 'interests of the supplier of the information', where supply was voluntary;
- commercial confidentiality;
- the protection of the environment.

In addition:

- Information about the applicant (personal information) will be dealt with under the Data Protection Act 1998. Personal information about a third party will be exempt if releasing it would breach the data protection principles.
- Only a limited number of exceptions can be claimed when the information requested relates to emissions.

Our powers of enforcement

The ICO enforces the Environmental Information Regulations. The enforcement provisions in the regulations are taken directly from the Freedom of Information Act 2000. We cannot intervene in any disputes that began under the 1992 Regulations. For more information on our enforcement powers, see page 11.

3. Data Protection Act 1998

Overview of the Act

- Came into force on 1 March 2000, repealing the Data Protection Act 1984.
- It does not seek to guarantee personal privacy at all costs, but to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.
- Applies to some paper records as well as computer records.
- Derived from EU Directive 95/46/EC which requires "Member States to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data".

Rights under the Act

- **The right to access**
  This allows individuals to find out what information is held about them on computer and in some manual records. This covers a wide variety of information, for example medical records, files held by public bodies, and financial information held by credit reference agencies.
- **The right to prevent processing for direct marketing**
  This means a data controller is required not to process information about individuals for direct marketing if asked not to. Everyone has the right to stop unwanted marketing offers being made to them.

- **The right to compensation**
  This allows individuals to claim compensation through the courts from a data controller for damage and, in some cases, distress caused by any breach of the Act.
- **The right to correction, blocking, removal and destruction**
  This allows individuals to apply to a court to order a data controller to correct, block, remove or destroy personal details if they are inaccurate or express an opinion based on inaccurate information.
- **The right to ask the ICO to assess whether the Act has been breached**
  This allows individuals to ask us to assess whether a data controller has breached the Act.
- **Rights in relation to automated decision-taking**
  This means that in some circumstances individuals can object to data controllers making significant decisions about them, such as their performance at work or creditworthiness, where the decision is completely automated and there is no human involvement.
- **The right to prevent processing**
  This means individuals can ask a data controller not to process information about them that causes substantial and unwarranted damage or distress. The data controller is not always bound to act on the request.

The data protection principles

Anyone processing personal information must comply with eight enforceable principles of good information handling practice. The data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept longer than necessary;
- processed in accordance with the individual's rights;
- secure;
- not transferred to countries outside the European Economic Area, unless there is adequate protection.

Notification

The 1998 Data Protection Act requires every data controller who is processing personal information electronically to notify us that they are doing so, unless they are exempt. Notification is the process by which a data controller's details are added to a public register of data controllers, which we maintain. A two-tiered notification fee structure was introduced on 1 October 2009. The two-tiered structure is based on an organisation's size and turnover. A data controller will need to assess which tier they fall in and hence the fee they are required to pay. The fee for tier 1 is £35 and the fee for tier 2 is £500. More information on tiered fees can be found in our guide 'Notification Fee Changes – what you need to know'.

Subject access request

Under the Data Protection Act, individuals can ask to see what information is held about them on computer and in some paper records, by writing to the person or organisation they believe is processing the data. This is called a subject access request.

In most cases, the maximum fee for a subject access request will be £10, but this can vary, particularly if the information is health or educational records. A request must include enough information to prove the applicant's identity and enable the information to be easily found.

The applicant must be given a reply within 40 days as long as the right fee has been paid. A data controller should act promptly in requesting the fee or any more information it needs to fulfil the request. If a data controller is not processing the applicant's personal information, it must reply saying so.

The fee for a subject access request to a credit reference agency is £2, and the information must be provided within seven working days.

Our duties and enforcement powers

- Promoting good information handling.
- Distributing information on data protection.
- Developing or approving codes of practice for data controllers.
- Serving information notices: requiring a data controller to provide us with specified information within a certain time period.
- Conducting assessments of compliance.
- Serving enforcement notices where there has been a breach that requires a data controller to take specified steps or stop taking steps in order to comply with the law.
- Issuing monetary penalties notices, requiring organisations to pay up to £500,000 for serious breaches of the Act (Data Protection only).
- Prosecuting those who commit criminal offences under the Act.
- Reporting directly to Parliament.

Appeals against notices can be heard by the First Tier Tribunal.

Civil monetary penalties

The ICO's power to issue monetary penalties came into force on 6 April 2010, allowing the ICO to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act. This power can be used as both a sanction and a deterrent against data controllers who deliberately or negligently disregard the law.

Criminal offences

A data controller who persistently breaches the Act and has been served with an enforcement notice can be prosecuted for failing to comply with a notice. This offence carries a maximum penalty of a £5,000 fine in the magistrates' court and an unlimited fine in the Crown Court.

Notification offences: unless exempt a data controller can be prosecuted if they fail to notify us about data processing they are doing or of any changes to that processing. Failure to notify is a strict liability offence. Being unaware of the law is not an excuse.

Unlawful obtaining or disclosing of personal information: it is a criminal offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal information, without the consent of the data controller.

If someone has obtained personal data illegally, it is an offence to sell it or to offer to sell it.

Data Protection Act scams: there have been many complaints surrounding companies claiming to be Data Protection Act or CCTV 'notification agencies'. These companies encourage firms to pay them large amounts to notify with the ICO, or risk large fines.

4. Privacy and Electronic Communications Regulations 2003

Overview of the regulations

These regulations apply to sending unsolicited marketing messages electronically such as by telephone, fax, email and text.

These regulations implemented the EU Privacy and Electronic Communications Directive, updated to include new rules on the use of the latest technologies in unsolicited marketing.

The directive includes rules on dealing with unsolicited email ('spam').

Rights under the Regulations

- Unsolicited marketing material sent by automated direct-marketing phone calls must have the prior consent of the subscriber, and must include the caller's identity.
- With non-automated direct-marketing phone calls, subscribers must be able to opt out of receiving them. Those on the Telephone Preference Service (TPS) register should not receive any such calls unless they give permission.
- Businesses may register with the TPS to prevent unsolicited marketing calls.
- Individuals and businesses can register their objection to receiving unsolicited direct marketing faxes by registering their number with the Fax Preference Service.
- Unsolicited marketing material by electronic mail (including text and picture messaging and emails)

should only be sent if the individual has opted in to receive them, unless the individual's email address was obtained in the context of a commercial relationship. The individual should always be given the opportunity to opt out of receiving the emails.

We are working with our European counterparts and the US to try to reduce spam. These regulations only apply to spam sent from within the EU. There is currently no legislation to cover spam sent to business addresses.

Individuals' rights

Individuals have the right to refuse unsolicited marketing communications through fax, phone, email and text messages.

Individuals have the right to complain to us if unsolicited marketing information continues to arrive after they ask for it to stop.

Organisations and individuals may also sue for breaches of the regulations if they can prove damage.

We have published guidance on the Privacy and Electronic Communications Regulations (available on the ICO website www.ico.gov.uk).

Anyone who signs up to the Telephone Preference Service (TPS) should be removed from cold-calling databases. The TPS is independent of the ICO. For more information contact:

Telephone Preference Service, DMA House, 70 Margaret Street, London, W1M 8SS

t: 0845 070 0707 **f:** 0207 323 4226
e: tps@dma.org.uk **w:** www.tpsonline.org.uk

Privacy and Electronic Communications Regulations 2011

On 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 came into force.

The Information Commissioner already had enforcement powers under the 2003 Regulations to serve enforcement notices for beaches of the Regulations, but the 2011 amendments have enhanced these powers and introduced new requirements.

The new powers enable the Commissioner to:

- impose civil monetary penalties of up to £500,000 for serious breaches of PECR;
- audit the measures taken by a provider of public electronic communications services (a service provider) to:
  - safeguard the security of that service
  - comply with the new personal data breach notification and recording requirements
- impose a fixed monetary penalty of £1,000 on a service provider that fails to comply with the new breach notification requirements; and
- require a communications provider to provide him with information needed to investigate the compliance of any person with PECR (a third party information notice).

The revised rules also cover technologies for storing information online, in particular cookies - a small file of letters and numbers that is downloaded on to your computer when you visit a website. In most cases websites wanting to use cookies must now get your consent. As organisations start to comply with these rules you are likely to start to see more information about cookies on sites and be given more choices about these cookies. This might include, for example, being asked to agree to a cookie being used for a particular service, such as remembering your preferences on a site.

At a glance overview

Your questions	Personal information (Data Protection Act and Privacy and Electronic Communications Regulations)	Official information (Freedom of Information and Environmental Information Regulations)
Can I ask to see personal information held about me by organisations and public authorities?	Yes This is known as making a 'subject access request'.	No It applies to all organisations that hold personal information, such as government departments, banks, credit card companies, local councils, schools, hospitals, doctors, your past and present employers, internet and mail order companies. It does not provide you with the right to access your personal information.
Can I request non-personal information held by public authorities and government departments?	No It only gives you the right to access personal information held about yourself.	Yes This right is known as the 'right to know'. It gives everyone the right to request recorded information held by public bodies. The Environmental Information Regulations also give additional rights to access information about the environment which is held by public authorities.

What type of information can I ask to see?	Using your right to subject access you can see information held about you, such as your medical records held by your doctor or hospital. You can also access your credit reference file – this will give you information about your credit history, which affects your credit rating.	Using your 'right to know' you can request any recorded information held by a public authority, such as decisions about local hospitals, money raised from car parks, or conviction rates for particular offences. Public authorities will also make information readily available via their publication schemes, for example minutes of meetings and annual reports.
How do I ask for the information?	In writing or by email, stating your full name and any names you may have been known by (for example, your maiden name) and your full address including postcode. An organisation can ask you for relevant information that will help them identify you and find the information you want.	In writing or by email, stating your name and an address to reply to, and clearly describing the information you want. It helps the organisation if you say you are making the request under the Freedom of Information Act or the Environmental Information Regulations. Requests made under the Environmental Information Regulations can also be made verbally.

Can I correct the information held?	Yes The Data Protection Act aims to ensure that your personal information is relevant, accurate, and up to date. If you believe and can prove that factual information held about you by an organisation is wrong, you can write to them stating who you are, what personal information is wrong and what should be done to correct it.	No The Freedom of Information Act only allows you to access information that is not personal to you. It does not require the public authority to take into account any comments you may make about its accuracy.
Can I stop my personal information being used for unwanted marketing?	Yes The Data Protection Act allows you to ask organisations to stop using your personal information for direct marketing purposes. The Privacy and Electronic Communications Regulations also give you rights to limit electronic direct marketing messages, including phone calls, faxes, emails and text messages. Read more on how to stop unwanted junk mail and spam.	Not applicable

Do I have a right to see information about someone else?	Normally, no	Yes, sometimes In certain circumstances you can. These include when you are legally responsible for another person, for example a parent for an infant, or when holding legal power of attorney for an elderly relative. You can request it, but many types of personal information don't have to be given to you.
Does the organisation have a time limit to reply to my request?	Yes Organisations must reply to a subject access request promptly and at most within 40 calendar days. A credit file should be supplied in seven calendar days.	Yes Organisations must reply to your request for official information within 20 working days.
Will I be charged for the information?	Possibly Most organisations are allowed to charge a maximum of £10. For some information such as health records you may be charged £50. A copy of your credit file will cost only £2.	Possibly In most cases the information will be provided free. But some costs, such as photocopying and postage, can be charged for. If a public authority has specific permission to charge for a particular type of information, it can ask you to pay these fees.

Will I always get all the information I ask for?	No You may be refused all or some of your personal information, if there is a good reason for doing so. For example, if the information you are requesting is subject to a criminal investigation or the information can identify a third party who does not want their information disclosed.	No Information must be disclosed unless there is a good legal reason not to. If you are refused information, the authority must explain why. Some information may be refused on the grounds of cost.
Can I get help if I feel my rights have been breached?	Yes If you have contacted the organisation or public authority but have been unable to solve the problem, we may be able to help.	

Explanation of terms

Data controller (Data Protection Act)
A person who either alone or together with others decides why and how personal information is to be processed. The data controller may be an individual or organisation.

Data processor (Data Protection Act)
A person who processes personal information on a data controller's behalf. This includes anyone responsible for disposing of confidential waste.

Data protection principles
Eight principles of good practice for processing personal information (see page 26).

Data subject (Data Protection Act)
The living person who is the subject of the personal information (data).

Decision notice
A decision notice sets out the Information Commissioner's final decision as to whether or not a public authority has complied with Freedom of Information Act or the Environmental Information Regulations with regard to specific complaints. Decision notices are drafted by case officers in the first instance, and signed off by a Deputy Commissioner or the Commissioner, or a member of the Commissioner's staff with delegated authority.

Enforcement notice (Data Protection Act)
The Information Commissioner has the power to serve an enforcement notice if he is satisfied that a data controller has contravened or is contravening the data protection principles. The notice must state what the data controller must do to comply with the Act. The data controller may appeal to the First Tier Tribunal, which may confirm, amend or overturn the notice. If there is no appeal and the data controller fails to comply with a notice, it is committing a criminal offence.

Enforcement notice (Freedom of Information Act)
The Information Commissioner has the power to serve an enforcement notice if he is satisfied that a public authority has failed to comply with any of the requirements of Part 1 of the Act.

First-Tier Tribunal (Informations rights)
The First-Tier Tribunal hears appeals by data controllers against notices the Information Commissioner has issued to them under the Data Protection Act. It also hears appeals by a public authority against enforcement notices and information notices under the Freedom of Information Act and appeals from a complainant or a public authority against decision notices.

Information notice (Data Protection Act and Freedom of Information Act)
A written notice from the Information Commissioner to a data controller or public authority asking for information he needs to carry out his functions. Failure to comply with an information notice is an offence.

Mailing Preference Service (Data Protection Act)
The Mailing Preference Service (MPS) is a non-profit-making body set up by the direct marketing industry to help people who do not want to receive junk mail.

The MPS will place an individual's surname and address on their consumer file, which is then made available to members of the direct marketing industry who subscribe to the MPS scheme. They promise to ensure that any names and addresses that appear on the MPS file are removed from the mailing lists they use and supply.

Notification (Data Protection Act)
Notification is the process by which a data controller's processing details are added to our public register. Under the Data Protection Act every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the data protection principles. The Commissioner maintains a public register of data controllers, available at www.ico.gov.uk. A register entry only shows what a data controller has told the Commissioner about the type of data being processed. It does not name the people about whom information is held.

Personal data
Personal data means information about a living individual who can be identified from that information and other information the data controller has or is likely to have in the future.

Practice recommendation (Freedom of Information Act)
When a public authority has not conformed with the provisions of the Codes of Practice, the Commissioner may issue a practice recommendation that identifies which areas of the Code have been breached and the steps necessary to conform. Practice recommendations are intended to promote good practice rather than compliance and as such are non-enforceable.

Processing (Data Protection Act) Processing means obtaining, recording or holding data or carrying out any operation or set of operations on data.

Public authority (Freedom of Information Act)
Any body, person or holder of any office listed in Schedule 1 of the Freedom of Information Act or designated by order and wholly owned companies as defined in section 6 of the Freedom of Information Act. Examples of some of the public authorities covered by the scheme are government departments, local authorities, NHS bodies (hospitals, doctors, dentists, pharmacists and opticians), schools, colleges and universities, the police, the House of Commons and the House of Lords, the Northern Ireland Assembly and the National Assembly for Wales.

Publication schemes (Freedom of Information Act)
The Freedom of Information Act places a duty on public authorities to adopt and maintain a publication scheme that must be approved by the Information Commissioner. The scheme commits an authority to routinely provide certain classes of information, it details how such information should be made available and when a charge can be levied. It also obliges authorities to produce and publish a 'guide to information' detailing the information the authority holds and makes available under each class heading, the manner in which it will be provided and, where a charge is to be made, what the cost will be.

Redacted information
Information which has been deleted or blanked out from a document because it is legitimately exempt from release.

Subject access request (Data Protection Act)
Under the Data Protection Act, individuals can ask to see what information is held about them on computer and in some paper records, by writing to the person or organisation they believe is processing the data. This is called a subject access request.

Telephone Preference Service and Fax Preference Service (Data Protection Act)
The Telephone Preference Service (TPS) and Fax Preference Service (FPS) are suppression schemes similar to the Mailing Preference Service (MPS). Organisations that engage in unsolicited direct marketing by telephone and fax must not contact individuals who have registered with these opt-out schemes. Registering with the TPS and FPS can help to reduce the number of unwanted telesales calls and marketing faxes an individual receives.

Vexatious complaints (Freedom of Information Act)
Under section 14(1) a public authority has no obligation to comply with a vexatious request. Vexatious requests are those that are obsessive, create disruption, harassment or have no serious purpose or value.

If you would like to contact us please call 0303 123 1113

www.ico.gov.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

August 2012

Information Commissioner's Office

Upholding information rights