

# Protecting privacy – promoting openness





# About the ICO

## Our mission

- 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. It aims to make public sector bodies more open and accountable. It also helps 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 another way for the public to access environmental information. The Regulations 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. It 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.

## Our vision

- By 2012, we will be recognised by our stakeholders as the authoritative arbiter of information rights, delivering high-quality, relevant and timely outcomes, responsive and outward-looking in our approach, and with committed and high-performing staff – a model of good regulation and a great place to work and develop.

## Our approach

In achieving our mission we aim to be a strategic regulator. This means making the best use of our resources by taking selective action where we can make the biggest difference.

In doing so, we believe that complying with the law is not a goal in itself. The benefits of freedom of information and data protection can, and should, be achieved without our constant intervention. So we encourage organisations to strive for good practice as a matter of self interest and good business practice, and aim to minimise the cost and complexity of compliance. We also take a targeted approach to enforcement, focusing on breaches where the risk of harm to individuals is greatest and being tough on those who deliberately or persistently fail to deliver the benefits the law intends.

We focus on four main goals:

- Educating and influencing
- Resolving problems
- Enforcing
- Developing and improving

# 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 12).

Any individual or organisation can request any information in writing, held by a public authority.

The public authority must tell the applicant within 20 working days if they hold the information and, unless the information is exempt, provide the information. 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 non-personal 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 7).

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 act on our conclusions (see 'enforcement powers' on page 10). If the applicant or the public authority is unhappy with our decision, they can complain to the Information Tribunal. The Information 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

### Responding to requests for information

Public authorities must 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 their time for considering release of the information to 40 working days. They must inform the applicant that they are doing this and give an estimated time for response.

Public authorities cannot normally charge a fee for supplying information in response to a request. However, they can estimate the cost of providing the information. If that cost exceeds a set limit, they do not have to comply with the request. The limit is £600 for government departments and £450 for all other authorities.

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

The applicant may ask to inspect the record on site. If a public authority has grounds for not releasing the information requested, 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;
- the internal appeals process;
- the applicant's right to complain to us.

## 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 must 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.

## The public interest

Public authorities need not disclose any information covered by one or more of the exemptions (see page 9). Some of these must be complied with by law. However, for most of them, 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.

## The exemptions

- There are 23 exemptions in the Freedom of Information Act, divided as follows:
  - Those that apply to a whole category (or class) of information, for example:
    - information about investigations and proceedings conducted by public authorities;
    - court records;
    - trade secrets.
  - Those that are subject to a ‘prejudice’ test, for example, where disclosure would, or would be likely to, prejudice:
    - the interests of the United Kingdom abroad;
    - the prevention or detection of crime; or
    - the activity or interest described in the exemption.
- The public interest test applies to most exemptions. These are called qualified exemptions. Those to which the test does not apply are called absolute exemptions.
- Exemptions for personal information:
  - If personal information relates to the applicant, the request must be addressed as a ‘subject access request’ made under the Data Protection Act 1998.
  - If the information requested relates to a third party, a decision on whether to release it will be based on the Data Protection Act.

When refusing a request for information, an authority cannot withhold an entire document because 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.

When refusing information an authority must explain which exemption or exemptions they have applied, why they have applied them and, where appropriate, fully explain the public interest factors for and against disclosure.

## The ICO's role and enforcement powers

Our approach is to be reasonable, responsible and firm, recognising that greater openness should strengthen government. This is done through:

- promoting good practice by public authorities in observing the Act;
- informing the public about the Act;
- developing, approving and maintaining the model publication scheme;
- monitoring the way the model publication scheme is adopted and operates;
- considering complaints about any alleged failure to comply with the Act or conform to the codes of practice;
- recommending that an organisation changes the way it handles requests or manages its records;
- issuing to public authorities notices such as:
  - **information notice** – requiring more information about a case;
  - **decision notice** – decision on a case;
  - **enforcement notice** – directing an organisation to amend its practices;
  - **practice recommendations** – not statutory or enforceable but can be issued to a public authority when they are in breach of either codes of practice.

If the applicant or public authority disagrees with our formal decision, they have 28 days to appeal to the independent Information Tribunal.

All notices may be appealed to the independent Information Tribunal, a practice recommendation cannot be.

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'. 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.
- Location of 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 also 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, for example companies involved in energy, water, waste and transport).

The definition of environmental information includes information on the state of the elements of the environment, such as:

- air, water, soil, land, flora and fauna (including people);
- emissions and discharges (gases and fluids), noise, energy, radiation, waste and other such substances;
- 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, contamination of the food chain; and
- cultural sites and built structures (as they may be affected by environmental factors).

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

All the exceptions are subject to the public interest test (see page 16). Public authorities must still disclose unless the public interest positively favours the exception in the particular case.

Public authorities must respond in writing within 20 working days.

An authority may charge for providing the information (see page 15).

The Environmental Information Regulations can be backdated to cover all information, not just information filed since they came into force.

## Rights under the Environmental Information Regulations

The Environmental Information Regulations create a strong 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 must aim to meet the applicant's requirements for information, and the format they prefer to receive it in, if stated.

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 act on our conclusions (see enforcement powers, page 17).

An applicant who is unhappy with our decision can appeal to the Information Tribunal.

## Responsibilities for public authorities

### ■ Actively making information available

- Public authorities must make their environmental information available increasingly through electronic means, such as via the internet.
- Public authorities must also organise their environmental information so that it can be systematically made public.

- There are minimum criteria as to what public authorities are expected to actively make generally available. These are stated in Article 7(2) of the European Directive (2003/4/EC).
- Public authorities that are also subject to the Freedom of Information Act can use their publication scheme as a way of complying in part with their responsibilities to actively make available their environmental information to the public.
- Public authorities must publish a scale of 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 can only be extended (to 40 working days) if a large volume of information is requested and it 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 registers or lists or for viewing at the public authority's premises. There is no 'appropriate limit' to the cost of providing environmental information.

If the public authority refuses access to information, it must explain which exception applies and whether the public interest in maintaining the exemption outweighs the public interest in releasing the information. It must also inform the applicant of their right to complain.

## 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 the public interest test. This means that the authority must explain to the applicant why, in all the circumstances of the case, the public interest in maintaining the exception outweighs the public interest in disclosing the information. 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

These include denying disclosure 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 proof of 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 may 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 10.

## **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, so 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 broken**

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 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. This currently costs £35 each year and should be done direct through us. 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**'.

## 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.
- Prosecuting those who commit criminal offences under the Act.
- Reporting directly to Parliament.

Appeals against notices can be heard by the Information Tribunal, an independent body set up to hear cases about enforcement notices or decision notices issued by us.

## 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.

### Examples

- In March 2009 Mr Thusita Weerakoon of Weerakoon Solicitors was fined £100 and ordered to pay £717.05 costs for failing to notify as a data controller under the Data Protection Act.
- Ian Kerr of Droitwich was fined £5,000 for failing to notify as a data controller. We investigated Mr Kerr after finding that he was running a secret operation to vet construction workers for employment in the industry.

**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.

## Example

- Two private investigators, Christopher Hackett, trading as Swift Investigations, and Darren Whalley of Managed Credit Services Ltd (MCS Ltd), were convicted in 2008 of unlawfully obtaining and selling personal information at Wimbledon Magistrates' Court, and fined £400 and £500 respectively. Each was also ordered to pay £400 towards prosecution costs. They managed to obtain individuals' personal details from BT and then traded the information unlawfully.

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.

- Two people were sentenced to a total of six and a half years' imprisonment in December 2004 after pleading guilty to conning businesses across the UK out of nearly £700,000 in data protection scams.

## 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 Act

- 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.

### Example

- Robert Logan, Director of Clear Debt Solutions, pleaded guilty to 13 offences relating to breaches of the Privacy and Electronic Communications Regulations in April 2009. Mr Logan was fined and ordered to pay costs of £6,274.53 after bombarding individuals and businesses with unwanted faxes. The action came after over 500 complaints to us and the Fax Preference Service.

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 website).

Anyone who signs up to the 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: 0845 070 0706  
e: [tps@dma.org.uk](mailto:tps@dma.org.uk)  
w: [www.tpsonline.org.uk](http://www.tpsonline.org.uk)

## **Our powers of enforcement**

We can serve an enforcement notice where an organisation is in breach of the regulations.

Breach of an ICO enforcement notice is a criminal offence subject to a fine of up to £5,000 in a magistrates' court, or an unlimited fine in the Crown Court.

# 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 19).

## **Data subject (Data Protection Act)**

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

## **Decision notice (DN)**

A DN sets out the Information Commissioner's final assessment as to whether or not a public authority has complied with FOIA or the EIR with regard to specific complaints. DNs are drafted by case officers in the first instance, and signed off by an Assistant Commissioner, Deputy Commissioner or the Commissioner.

### **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 Information Tribunal, which may confirm, amend or overturn it. 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 respond properly to a request for information.

### **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.

### **Information Tribunal (Data Protection Act and Freedom of Information Act)**

The Information 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.

### **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 wish 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](http://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**

When a public authority has not conformed with the provisions of the Codes of Practice, the Commissioner may issue a non-legally-enforceable Practice Recommendation which identifies the Code breaches and the steps necessary to comply. Practice Recommendations are intended to promote good practice rather than compliance.

### **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 organisation, any person, or the holder of any office listed in the Freedom of Information Act, or designated by order, and publicly owned companies. 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, 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 lists and defines the classes of information that will be published, indicates how information is or is intended to be published, and states whether charges apply to supplying the information.

### **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 the information about them that is held 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.

### **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 reduce unwanted telephone sales calls or marketing faxes an individual receives.

### **Vexatious complaints**

Vexatious complaints are those that are obsessive, create disruption, harassment or have no serious purpose or value. Section 50(2)(c) of the Freedom of Information Act gives the Commissioner discretion not to investigate complaints that are 'vexatious' or 'frivolous'. Section 14(1) of the Freedom of Information Act gives public authorities discretion not to provide information in response to applications that are 'vexatious' or 'repeated'.

## Contact us

If you would like to contact us please call 08456 306060  
or 01625 545 745 if you would prefer to call a national rate number.

e: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)

w: [ico.gov.uk](http://ico.gov.uk)



October 2009

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



Information Commissioner's Office