Personal information toolkit

Advice on how to safeguard your personal information

ico.

Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

We do this by promoting good practice, ruling on eligible complaints, providing guidance to individuals and organisations, and taking action when the law is broken.

The ICO enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations.

- 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 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 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.
- 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 Infrastructure for Spatial Information in the European Community Regulations 2009 gives the Information Commissioner enforcement powers in relation to the pro-active provision by public authorities of geographical or location based information.

This leaflet gives you advice and tips on how to manage and safeguard your personal information.

The leaflet explains how you can:

Protect your personal information 7

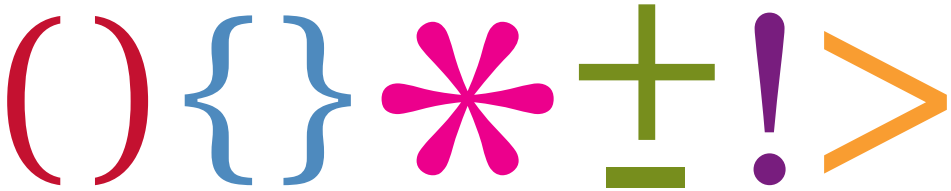
Access your personal information 11

Correct your personal information 17

Reduce unwanted sales calls, junk mail and electronic marketing 19

Recognising the signs of identity theft 29

Make sure your personal information moves with you 35



What is personal information?

Personal information is information about you. It can be your name, address, or telephone number. It can also be the type of job you do, the things you buy when you are shopping and the place you went to school.

Why is managing my personal information important?

Today, like it or not, our personal information is held by many public and private organisations.

These may include:

- government departments
- gas, electric, phone and internet service providers
- employers
- mail-order and internet companies
- schools
- local councils
- banks and building societies
- supermarkets and high-street retailers
- hospitals and doctors
- the police
- airlines and travel agents

What is my personal information used for?

Every day, you will give out your personal information in some way or other. It could be when you are shopping and you claim loyalty points, or in your workplace, or when you carry out a transaction with your bank.

But have you ever really thought about who you are giving your personal information to and what they will use it for?

Although most of the personal information stored about you will provide benefits like better medical care and financial reassurance, it also brings dangers. If your personal information is wrong, out of date or not held securely, it can cause problems. You could be unfairly refused a job, benefits or credit, or a place at college. In extreme cases, you could be a victim of identity theft or arrested for a crime you did not commit.

So what are my rights?

The Data Protection Act allows you to see information held about you and get it corrected if it is wrong. Organisations that hold your personal information must use it fairly, keep it secure, make sure the information is accurate and keep it up to date.

The Act also gives you the right to stop your personal information being used for unwanted marketing.

The Privacy and Electronic Communications Regulations give you the right to stop electronic direct-marketing messages, including phone calls, faxes, emails and texts.

If you think an organisation may have breached the Data Protection Act in the way it holds and handles your personal information, you can complain to the Information Commissioner's Office.

For advice on how to complain, visit **www.ico.gov.uk** or telephone our helpline on 0303 123 1113.

Protect your personal information

Your personal information is valuable. Treat it as you would any valuable item

Protecting your personal information

Your personal information is valuable, so you should treat it just as you would any valuable item.

With crimes like identity theft increasing, it is even more important for you to safeguard your information. Criminals can find out and use your personal details to open bank accounts, apply for credit cards and loans and get state benefits in your name.

Don't panic – there are some simple steps you can take to safeguard your information:

- ☐ Store in a safe place any documents carrying your personal details, such as your passport, driving licence, bank statements and utility bills.
- ☐ Shred or destroy personal documents you are throwing away such as bills, receipts, bank or credit-card statements and other documents that show your name, address or other personal details.
- ☐ If you have to post personal documents, ask the post office for advice on the most secure method.
- ☐ Limit the number of documents you carry around that contain your personal details. If possible, don't leave personal documents in your vehicle.
- ☐ Check your bank and credit card statements regularly for unfamiliar transactions.
- ☐ Use different passwords and PINs for different accounts and take extra care when using public computers to access your personal information.
- ☐ Regularly get a copy of your personal credit file to check for any suspicious credit applications. For more information on how to do this, see our website www.ico.gov.uk or ring 08453 091 091 for a free copy of 'Credit explained'.
- ☐ Always think about who you are giving your information to. Be cautious about providing any personal details to unsolicited callers by phone, fax, post, email or in person, unless you are sure the person is who they say they are. If you are suspicious, ring the organisation back on an advertised number or visit their website.
- ☐ Even if you know who is asking for your information, think twice before you answer their questions. If it's not clear why they need the information, ask them or just move on to the next question.
- ☐ Ensure your home computer is protected before you go online – buying a good anti-virus, firewall and anti-spam software package will protect your computer against viruses and any spyware software, which can be used to obtain your personal information.

- ☐ Secure your WiFi. If your WiFi network is not secured, anyone within range can connect to it. An unsecured wireless network is open to hackers to gain access to your personal information. When you buy a wireless router, or if you already have a wireless network installed, make sure you protect yourself by enabling its security features.
- ☐ Do not click on links to go to a website unless you can be confident it is genuine.
- ☐ If you use a central or communal postal-delivery point, such as in a block of flats, make sure you have a lockable postbox and collect your post as soon as possible. If your mail regularly fails to arrive, report this to Royal Mail.
- ☐ If you move house, redirect all your mail and inform your bank, utility companies and other organisations of your new address. You can find more information on safeguarding your mail on page 37.

Access your personal information

You have the right to access information that organisations hold about you

Accessing your information

You have the right to access information that organisations hold about you. Asking them for your information is known as making a 'subject access request'.

Who can I make a subject access request to?

You can make a subject access request to any organisation you believe holds information about you.

Examples include:

- banks and credit-card companies;
- hospitals and doctors;
- your present or past employer; and
- mail-order companies.

How do I make a subject access request?

To make a subject access request, write to or email the organisation you believe holds information about you. If you are not sure who to write to, address your letter or email to the company secretary of the organisation.

We give a sample letter overleaf.

Your letter should include:

- your full name – also give any names you used to be known by, such as a maiden name;
- your full address, including your postcode;
- any information you think the organisation will need to find your information and check that you are who you say you are. For example your employer may need your payroll number, and a hospital may need your NHS number;
- it is also advisable to refer to the Data Protection Act.

It is a good idea to send your request by recorded delivery. Keep a copy of the letter and any further letters you send or receive. The organisation may ask for a fee, which is normally no more than £10.

However, they may charge you more for certain types of information, such as health records. They may also ask for more information to check that you are who you say you are.

Once you have provided all the relevant information and fee, the organisation must reply within 40 days.

123 Any Street
Anytown
A45 6EC

28 January 2011

Dear Company Secretary

Under the Data Protection Act 1998, please send me a copy of all the information you hold about me.

If you need more information from me, or if you make a charge, please let me know as soon as possible.

If you do not normally handle these requests, please pass this letter to your Data Protection Officer or another appropriate person.

Yours faithfully

Adam N. Other

Adam Neil Other

The reply should include:

- a copy of all the information they hold about you;
- details of:
  - why your information is processed; and
  - the types of organisations it may be passed on to.

The information may be sent to you as a computer print-out, in a letter or on a form. You should be able to understand the information, and any codes should be explained.

You can also obtain a copy of your credit file. For more information on this, visit our website www.ico.gov.uk or phone 08453 091 091 to request a free copy of 'Credit explained'.

What information can't I see?

Some information on your record may be held back, for example if:

- it could identify someone else and that person objects to being identifed; or
- you are the subject of a criminal investigation.

Who do I contact if I have difficulty getting my information?

If you do not receive a reply to your request within 40 days, you should send the organisation a reminder by recorded delivery (again, keep a copy).

If you still don't receive a reply, visit our website **www.ico.gov.uk** or contact our helpline on 0303 123 1113 for advice on what to do next.

Correct your personal information

If personal information held on you is wrong, you have the right to have it corrected

Correct *

Correcting your information if it's wrong

If you believe your personal information is wrong, you should write to the organisation, to tell them what information you believe is wrong and what should be done to correct it.

There is no particular form of words you should use, but make clear the following:

- who you are and what personal information is wrong; and
- what should be done to correct it.

If you are sending a letter, it is advisable to send it by recorded delivery. You can also email your letter if the organisation can identify you and the personal information you are referring to from your email.

Keep a copy of what you send and any replies you receive. Record the dates of all correspondence.

Who do I contact if I have difficulty getting my information corrected?

If the organisation fails to correct the information on your request, you should write to them again, enclosing a copy of your original letter and requesting a response.

If they still refuse, or fail to deal with your request, visit our website **www.ico.gov.uk** or contact our helpline on 0303 123 1113 for advice on what to do next.

Reduce unwanted sales calls, junk mail and electronic marketing

Always tick the right box on any form you fill out

Reducing unwanted sales calls, junk mail and email marketing

One of the best ways to stop unwanted marketing is to tick the appropriate box on any form you fill out. When filling in any form, always read the short statement provided by the organisation collecting your information – this is normally at the bottom of the form and is sometimes indicated by this symbol 🔓.
The statement will summarise how the organisation intends to use your information. The statement will usually give you the option to either 'opt in' to or 'opt out' of having your information used for marketing or passed to a third party.

Even if you forget to tick the box, you always have the right to ask an organisation to stop using your personal information for marketing.

You can do this in a letter or email. There is no particular form of words you should use, but you need to make clear the following:

- your identity;
- the personal information you are referring to; and
- the method of direct marketing you wish to stop.

If you are not sure who to write to, address your letter or email to the organisation's data protection officer or company secretary. It is also advisable to send any letters by recorded delivery and keep a copy. When they receive your letter or email, the organisation should stop using your personal information for marketing. This should normally take no longer than 28 days. But it may take longer for pre-printed mailings.

Reducing sales calls

To reduce the number of unwanted sales calls, register your home and mobile phone numbers with the Telephone Preference Service (TPS). This service is free and takes 28 days to become active. Note that registering your mobile number with the TPS will only stop live marketing voice calls, not SMS text messages, or automated calls.

To stop unwanted sales calls, register your details:

online at
tpsonline.org.uk;

by phoning
0845 070 0707;

or by writing to:
The Telephone Preference Service (TPS)
DMA House
70 Margaret Street
London
W1W 8SS

If you have a business, you can also register your company's phone number(s) with the Corporate Telephone Preference Service (CTPS).
For more information on how to do this, visit www.tpsonline.org.uk/ctps/what/.

Reducing the number of silent calls

You can reduce silent calls made by automatic dialling equipment by registering your number with the Silent Callgard Service on 0844 372 2325. Silent calls do not fall under the Privacy and Electronic Communications Regulations as no marketing message is sent. For further advice about the rules on silent calls, visit the Ofcom website www.ofcom.org.uk.

Reducing the amount of fax marketing

As an individual or a business, you can also register your fax number with the Fax Preference Service to reduce the number of unwanted faxes you get. Again, this service is free, and can be done:

online at
fpsonline.org.uk;

by phoning
0845 070 0702;

or by writing to:
Facsimile Preference Service (FPS)
DMA House
70 Margaret Street
London
W1W 8SS

Who do I contact if I have difficulty stopping unwanted calls and faxes?

If, after you register with the TPS and FPS, you still continue to receive unwanted sales calls, visit our website www.ico.gov.uk or contact our helpline on 0303 123 1113 for advice on what to do next.

Reducing direct and junk mail

To reduce the volume of unwanted direct or junk mail, register your name and address with the Mailing Preference Service (MPS).

The MPS is a free service set up by the direct-marketing industry to help people who don't want to receive junk mail. The MPS can remove your name and address from up to 95% of direct-mail lists. However, it will not stop direct mail from companies who don't check their list with the MPS before sending direct mail, and it won't stop mail addressed to 'the occupier'. It will take up to four months for the service to take full effect, but you should notice a reduction of mail during this period.

To stop direct and junk mail:

register your details online at
www.mpsonline.org.uk;

phone
0845 703 4599;

or write to:
Mailing Preference Service (MPS)
DMA House
70 Margaret Street
London
W1W 8SS

You can also stop the amount of 'unaddressed mail' you receive by registering your address with the Royal Mail's Door to Door opt-out service. However, this service will not stop mail addressed to 'the occupier'.

To register write to:
Freepost RRBT-2BXB-TTTS
Royal Mail Door to Door Opt Outs
Kingsmead House
Oxpens Road
Oxford
OX1 1RX

Or email:
optout@royalmail.com

Who do I contact if I have difficulty stopping unwanted mail?

If you have registered with the MPS but are still receiving unwanted mail, you can complain directly to the MPS, who will investigate and contact the company sending the mail.

To complain, write to the MPS with a copy of the unwanted mail you have been sent, including the envelope, as this will help the MPS to identify the source of the mailing.

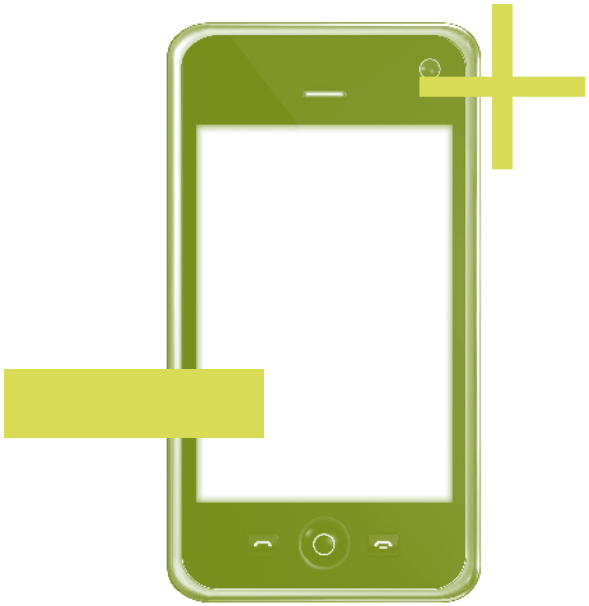
To complain, write to:
Mailing Preference Service
MPS Freepost LON20771
London
W1E 0ZT

If, after you register and complain to the MPS, you still continue to receive unwanted mail you should contact the company directly to complain. If after that they keep on sending you unwanted mail, visit our website www.ico.gov.uk or contact our helpline on 0303 123 1113 for advice on what to do next.

Electronic marketing

Electronic marketing includes any text, sound or picture messages that organisations send you electronically. This means the message you receive could be sent via email, text, or picture messaging. It enables organisations to deliver their marketing messages straight to your inbox.

The vast majority of responsible organisations who send you marketing using electronic methods will ask for your permission before they send it. This could be when they collect your information, but they should also give you an opportunity to opt out in every marketing email, text or recorded message they send you.



Spam

Spam is email that you don't want and didn't ask for, and its content can often cause embarrassment and distress. Most spam comes from outside the UK. If you are getting a lot of bulk spam from outside the UK, there is little help we can give you. However, you could speak to your internet service provider (ISP) for advice on spam filters, or visit our spam webpage at www.ico.gov.uk for more general advice.

You can take the following steps to reduce the amount of spam you receive:

- Be careful who you give your email address to.
- Consider having separate personal and business email addresses.
- Choose an email address that is difficult to guess.
- Don't advertise your email address.
- Check privacy policies and marketing opt-outs carefully.

Top tips for reducing spam

- Check privacy policies and marketing opt-outs or opt-ins carefully. When filling in any form, look out for the 'opt-in or opt-out' box, which is usually at the bottom of the form. If you read the short statement, it will tell you how the organisation intends to use your information.
- Never respond to spam. Replying can indicate that your email address is live. This can encourage the more unscrupulous senders to send you even more emails.
- Don't click on the adverts in spam emails. By clicking on spammers' web pages, you identify your email address as being live and may make yourself a target for more emails. It can also make your computer open to virus and other malicious attacks.
- Use a spam filter on your computer. Spam filters are programs that work with your email package to sift through new emails, identifying spam and blocking it.
- Keep your home computer well maintained. Hackers and spammers can exploit software problems, so most software companies issue product updates and patches that fix known problems. Download the updates and patches to ensure your computer is well protected.

Websites such as www.privacyrights.org and www.getnetwise.com also offer advice, although some of the advice is specific to US-based users.

Who do I contact if I have difficulty reducing the amount of electronic marketing I receive?

If, after you tell the organisation you want to 'opt out', you still continue to get unwanted electronic marketing, visit our website **www.ico.gov.uk** or contact our helpline on 0303 123 1113 for advice on what to do next.

Still receiving unwanted electronic marketing?
Visit our website www.ico.gov.uk or
contact our helpline on 0303 123 1113.

Recognising the signs of identity theft

Your identity is one of your most valuable assets

Recognise !

Recognising the signs of identity theft

Your identity is one of your most valuable assets. However, criminals can use a number of methods to find out your personal information and will then use it to open bank accounts, take out credit cards and apply for state benefits in your name. If your identity is stolen, you can lose money and may find it difficult to get loans, credit cards or a mortgage until the matter is sorted out.

You can find tips on protecting your personal information on page 6 of this leaflet.

Know the signs

There are a number of signs to look out for that may mean you are or may become a victim of identity theft. These include:

- You have lost or had important documents stolen, such as your passport or driving licence.
- Post from your bank or utility provider doesn't arrive.
- Items that you don't recognise appear on your bank or credit-card statement.
- You apply for state benefits, but are told you are already claiming.
- You receive bills or receipts for goods or services you haven't asked for.
- You are refused financial services, credit cards or a loan, despite having a good credit rating.
- You receive letters in your name from solicitors or debt collectors for debts that aren't yours.

Act quickly

If you think you are a victim of identity theft or fraud, act quickly to ensure you are not liable for any financial losses.

- If you believe that you are a victim of identity fraud involving plastic cards, online banking or cheques then you must report it to your bank as soon as possible. The bank will then be responsible for investigating the issue and will report any case of criminal activity to the police. The police will record the case and decide whether to carry out follow up investigations.
- If you think you are a victim of another type of identity fraud then you must report the matter to the relevant organisation. Depending on their advice you should then alert your local police force.
- Report all lost or stolen documents, such as passports, driving licences, credit cards and cheque books to the organisation that issued them.
- If you don't know which organisation to contact, you can call Action Fraud on 0300 123 2040 for advice.
- Inform your bank, building society and credit card company of any unusual transactions on your statement.
- Request a copy of your credit file to check for any suspicious credit applications.
- Contact CIFAS (the UK's Fraud Prevention Service) to apply for protective registration. Once you have registered you should be aware that CIFAS members will carry out extra checks to see when anyone, including you, applies for a financial service, such as a loan, using your address.

Once you have registered you should be aware that CIFAS members will carry out extra checks to see when anyone, including you, applies for a financial service, such as a loan, using your address.

Who do I contact for more advice on identity theft and fraud?

You can get advice on what to do if you become a victim of identity theft or fraud from:

CIFAS – The UK's Fraud Prevention Service

6th Floor - Lynton House
7 - 12 Tavistock Square
London
WC1H 9LT

www.cifas.org.uk

You can also get more advice at:

Fraud Reduction

www.fraud-stoppers.info

Home Office

www.identitytheft.org.uk

Bank Safe Online

www.banksafeonline.org.uk

Action Fraud

www.actionfraud.police.uk

Financial Services Authority

Telephone: 0845 606 1234

www.fsa.gov.uk

Financial Fraud Action UK

www.financialfraudaction.org.uk

To report the theft or loss of post and other important documents:

Identity and Passport Service

Telephone: 0300 222 0000

www.passport.gov.uk

Driver and Vehicle Licensing Agency

Telephone: 0300 790 6801

www.dft.gov.uk/dvla

Royal Mail

Telephone: 08457 740 740

Make sure your personal information moves with you

Failing to do so could leave you open to identity theft

Move

Making sure your personal information moves with you

Moving house can be very stressful, and redirecting your personal mail and bills maybe the last thing on your mind. However, redirecting your mail and informing your bank, credit- and store-card companies and utility providers of your new address is crucial to safeguard your personal information – failing to do it could leave you open to identity theft.

Top tip

Here is a list of the organisations you should give your new address to:

- banks and building societies
- credit- and store-card providers
- local council (for council tax and housing benefits)
- Department for Work and Pensions (for state benefit payment)
- DVLA (for vehicle registration and driving licence)
- gas, electric, phone and internet service providers
- TV Licensing
- doctor and dentist
- sports clubs
- loyalty card schemes
- optician
- any mail-order catalogues and magazine subscriptions.

Redirecting your mail

To redirect your mail, contact Royal Mail and they will help to ensure that when you move house, your mail moves with you. For a fee, Royal Mail can redirect your mail from any UK address to any other UK or overseas address, including British Forces and PO Box addresses. You can arrange to have your mail redirected for one to 12 months.

For more information on how to redirect your mail:

visit www.royalmail.co.uk; pick up a 'Moving home?' redirection application form at your nearest Post Office; or phone 08457 740 740.

Royal Mail can also help if you think your post is being stolen. They will be able to check whether a mail-redirection order has been made in your name without your knowledge.

Once you've moved

Once you have settled into your new home, you should consider checking that your personal information is still secure by getting a copy of your credit file two to three months after you move. You can also register your new address and phone number with the Mailing Preference Service and Telephone Preference Service; this will help to reduce the amount of unwanted marketing you get. We give details on how to do this elsewhere in this leaflet.

Who do I contact if I have difficulty with my post?

You should report the theft and loss of any post to:

Royal Mail

08457 740 740

Specialist tools

You will find more information in the 'Personal information' section of our website www.ico.gov.uk

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

January 2011

ico.

Information Commissioner's Office

Upholding information rights