

# Advice on how to safeguard your personal information



The Information Commissioner's Office (ICO) oversees the laws that give you rights about the personal information that organisations hold about you and makes sure this information is handled properly.

We have written this leaflet to give 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 If your personal information is wrong, out of date or not held securely, it can cause problems.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.org.uk](http://www.ico.org.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.
- ☐ Be careful when providing your personal information online. In particular, do not make too much personal information available to lots of people, for example

by having open access on social networking sites. For further information on this visit the online safety pages at our website **www.ico.org.uk**. Your personal information can be used to steal your identity and commit fraud. Be wary of anyone who asks for your bank or credit card details, and only use secure sites when shopping online – secure sites usually carry the padlock symbol.

- ☐ 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.org.uk** or ring 0303 123 1113 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.



---

## 10 Protect your personal information

---

- ☐ 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, and a contact telephone number; and
- 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 may be helpful to:
  - refer to the Data Protection Act;
  - make reference to the 40 day deadline; and
  - make reference to the assistance the ICO can provide.

It is a good idea to send your request by recorded delivery or email. Keep a copy of the correspondence and any further correspondence 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.



[Your full address]  
[Phone number]  
[The date]

[Name and address of the organisation]

Dear Sir or Madam

**Subject access request**

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the Data Protection Act 1998 relating to: [give specific details of the information you want, for example

- your personnel file;
- emails between 'A' and 'B' (between 1/6/11 and 1/9/11);
- your medical records (between 2006 & 2009) held by Dr 'C' at 'D' hospital;
- CCTV camera situated at ('E' location) on 23/5/12 between 11am and 5pm;
- copies of statements (between 2006 & 2009) held in account number xxxxx).]

If you need any more information from me, or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the Data Protection Act 1998 should be responded to within 40 days.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at [ico.org.uk](http://ico.org.uk)

Yours faithfully

[Signature]

## 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.org.uk](http://www.ico.org.uk)** or phone 0303 123 1113 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 identified; 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 or email (again, keep a copy).

You can find a non-response sample letter on our website, **[www.ico.org.uk](http://www.ico.org.uk)**.

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

[Your full address]

[Phone number]

[The date]

[Name and address of the organisation]

Dear Sir or Madam

### **Non response to a subject access request**

I am writing further to my letter of [date] in which I made a subject access request, because I have not received any response from your organisation.

As the statutory time limit for responding to my subject access request (40 days) has now expired, I would be grateful if you could provide a response as soon as possible.

If I do not receive a response from your organisation within 14 days, I will report this matter to the Information Commissioner's Office (ICO).

You can find advice on the ICO's website on how to deal with a subject access request [[ico.org.uk/sar](http://ico.org.uk/sar)] and information on their powers and the action they can take [[ico.org.uk/action](http://ico.org.uk/action)] or call them on 0303 123 1113.

\*If there is anything you would like to discuss, please contact me on the following [telephone number].

Yours faithfully

[Signature]

\*optional

# Correct your personal information

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



# 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. Provide documentary evidence of the inaccuracies where possible.

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.org.uk](http://www.ico.org.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](http://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/tps/whatiscorporatetps.html](http://www.tpsonline.org.uk/tps/whatiscorporatetps.html).

## Reducing the number of silent calls

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 contact Ofcom on 020 7981 3040 or visit [www.ofcom.org.uk](http://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](http://fpsonline.org.uk)**;

by phoning

**0845 070 0702**;

or by writing to:

**Fax 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.org.uk](http://www.ico.org.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](http://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 RSTR-YCYS-TGLJ**

Royal Mail Door to Door Opt Outs  
Kingsmead House  
Oxpens Road  
Oxford  
OX1 1RX

Or email:

**[optout@royalmail.com](mailto: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**

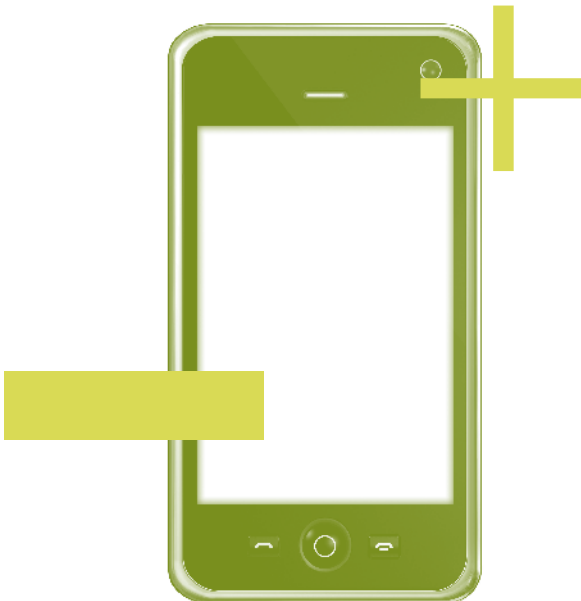
MPS Freepost LON20771  
London  
W1E 0ZT

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.org.uk](http://www.ico.org.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.

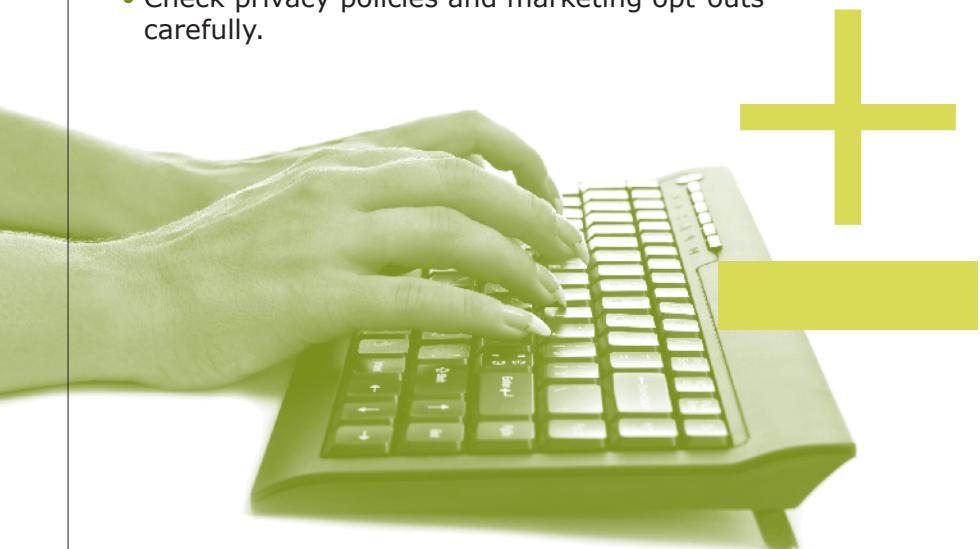


## Spam

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. As a lot of spam comes from overseas, the Information Commissioner has an agreement with a number of overseas bodies to cooperate and exchange information to try and stop spam emails that are sent from those places. To try to reduce the amount of spam you receive, you could speak to your internet service provider (ISP) for advice on spam filters, or visit our website **[www.ico.org.uk](http://www.ico.org.uk)** for more advice on spam.

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.

## 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.org.uk](http://www.ico.org.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.org.uk](http://www.ico.org.uk) or  
contact our helpline on 0303 123 1113.

Recognising the  
signs of identity theft  
Your identity is  
one of your most  
valuable assets

# 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 8 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.
- Mail 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.

- Report all lost or stolen documents, such as passports, driving licences, credit cards and chequebooks to the organisation that issued them.
- 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.
- Report the theft of personal documents and suspicious credit applications to the police, and ask for a crime reference number.
- 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.

## 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**

CIFAS – The UK's Fraud Prevention Service  
Capital House  
E-State  
Bankhead Crossway South  
Edinburgh  
EH11 4EP

Telephone: 0330 100 0180

[www.cifas.org.uk](http://www.cifas.org.uk)

You can also get more advice at:

### **Action Fraud**

Telephone: 0300 123 2040

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

### **CardWatch c/o APACS**

Mercury House  
Triton Court  
14 Finsbury Square  
London EC2A 1LQ

[www.cardwatch.org.uk](http://www.cardwatch.org.uk)

### **Financial Ombudsman Service**

Telephone: 0800 0 234567

[www.financial-ombudsman.org.uk](http://www.financial-ombudsman.org.uk)

### **Bank Safe Online**

[www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)

### **Financial Fraud Action UK**

[www.financialfraudaction.org.uk](http://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](http://www.passport.gov.uk)

### **Driver and Vehicle Licensing Agency**

Telephone: 0300 790 6801

[www.dvla.gov.uk](http://www.dvla.gov.uk)

### **Royal Mail**

Telephone: 03457 740 740

[www.royalmail.com](http://www.royalmail.com)

Make sure your  
personal information  
moves with you  
Failing to do so could  
leave you open to  
identity theft

# Making sure your personal information moves with you

---

Moving house can be very stressful, and redirecting your personal mail and bills may be 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 three, six or 12 months.

For more information on how to redirect your mail:

- visit [www.royalmail.com/redirection](http://www.royalmail.com/redirection);
- pick up a redirection application form at your nearest Post Office; or
- phone 03457 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**

03457 740 740

## Specialist tools

You will find more information in the 'Personal information' section of our website **[www.ico.org.uk](http://www.ico.org.uk)**





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

**[www.ico.org.uk](http://www.ico.org.uk)**

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

July 2015



Information Commissioner's Office

Upholding information rights