

Data protection

# Protecting your personal information online

**ico.**

Information Commissioner's Office

---

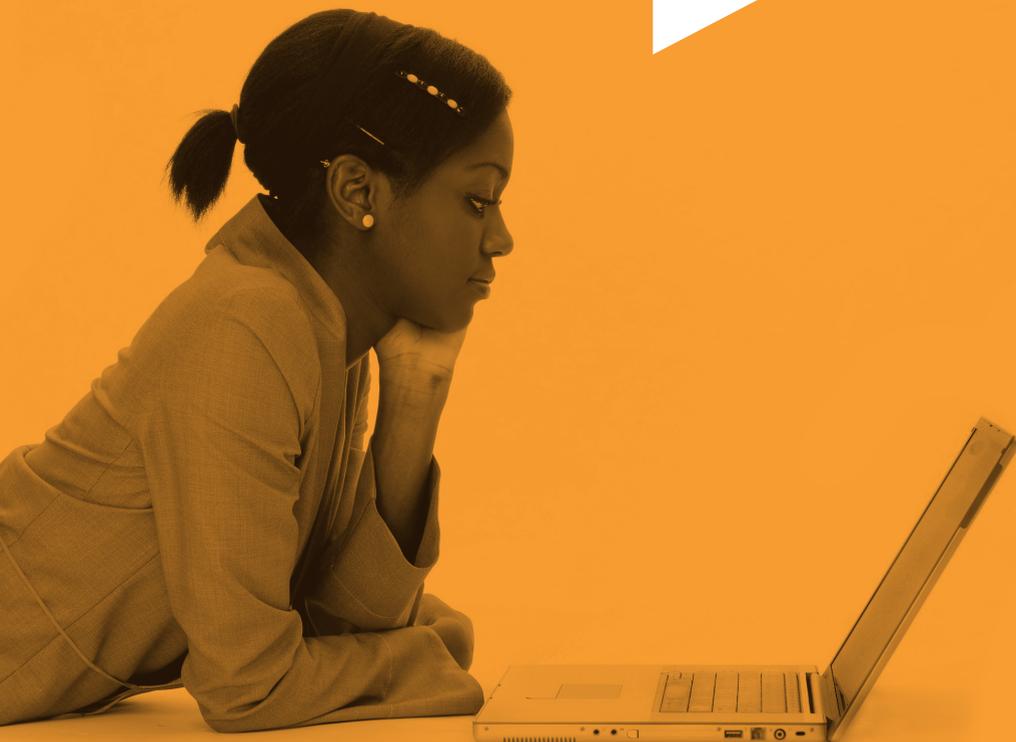
## Introduction

---

More and more people are conducting their personal affairs online. Online shopping, social networking, job hunting and the ability to carry out 'official' functions, such as renewing car tax or contacting local councils and government departments online, are now an everyday part of life. Doing things online can offer convenience and widen opportunities, and in general people value it.

Organisations that collect and use your information have responsibilities to protect it. However, you can take various precautions to protect yourself from identity fraud or the misuse of your information, or to ensure that your privacy is respected in the way you would want.

To help you navigate  
this book better look  
out for online links



## Protecting your personal information online

When doing any online transaction you can take steps to protect your personal information. Use the same common sense as you would when asked for personal information on paper or face to face. Ask yourself:

- who is collecting the information?
- is it necessary?
- what will be done with it?
- what are the consequences for me?

Check a site's privacy notice to find out what it intends to do with your information. A privacy notice, sometimes called a privacy policy or statement, should tell you who is collecting your information, what it is going to be used for, and whether it will be shared with other organisations.

If the intentions are not clear, ask the company concerned before you give any personal information, especially if it is sensitive. Companies may want to use your personal information to send you marketing or pass your details to other companies for marketing purposes. They should give you the chance to opt in or out of receiving such information.



## Protecting your identity online

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. 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.

Be careful when providing the following information:

- Full name
- Full address
- Date of birth
- Telephone number
- National insurance number
- School/workplace
- Birthplace
- Previous addresses.

When choosing a password, avoid 'obvious' choices such as mother's maiden name, child's name, pet's name, or other reference that someone may be able to find out through information you have posted elsewhere. Try to use random mixtures of numbers and letters. Use different passwords for different sites.

## Online scams and how to avoid them



Numerous scams are in operation to get you to provide personal details, including details of your bank account or credit card, for fraud. Phishing is a scam that lures you under false pretences to websites which look legitimate to get you to provide personal information. Such emails appear to be from recognisable sources such as banks but are actually linked to fraudulent websites.

- If in doubt, don't open emails or attachments.
- Before disclosing any personal information online, make sure you know who you are dealing with.
- Be suspicious of anyone who asks for your bank account or credit card details or asks for your password.
- Examine the email sender's address carefully before opening an email, and do not click on any links or email attachments unless you are sure of the sender's identity.

For more about protecting your personal information online, see:

<http://www.getsafeonline.org/>



## Online marketing and advertising

There are different ways of advertising to people online. Some involves displaying the same adverts to everyone who visits a particular website. 'Online behavioural advertising' involves showing a selection of adverts based on websites you have visited. This targeted approach aims to tell you about products or services you are likely to be interested in.

Organisations and companies have always used information about their customers to market goods and services to them. For many people this will be a welcome and useful feature of using the internet, particularly when shopping online. However, some people dislike this approach and don't want their buying or browsing habits used like this. Websites should provide an easy way for you to opt out of receiving such adverts or recommendations and should make clear to you how to disable cookies (see below) if you wish to do so.

The Internet Advertising Bureau provides information on how online behavioural advertising works, and gives links to several organisations that enable you to opt out of behavioural advertising.

<http://www.youronlinechoices.com/>



## Cookies – what they do and how to control them

---

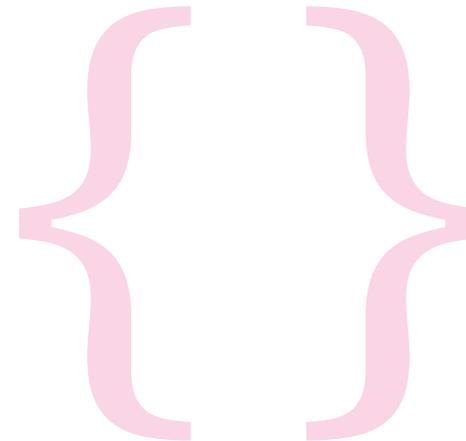
Cookies are files used by websites to collect information about your online activity. They can recognise your computer when you log on and can allow a website to store and remember usernames and passwords. For websites you use regularly, this can save you time. Some sites use cookies to send you targeted advertisements or offers, based on the websites you have visited.

All major browsers have cookie controls, which allow you to view and delete cookies or block them completely. Remember that blocking all cookies may mean you have to re-enter your login and password details when returning to familiar sites, and that some functions, such as shopping carts, may not work. Some cookie management tools allow you to selectively block cookies or receive warnings when a cookie is placed on your computer. You can use your cookie controls to strike the right balance between convenience and privacy.

## Browser privacy settings and security

---

Your internet browser – the software you use to browse the web, for example Internet Explorer, Firefox, Chrome or Safari – will have built-in tools to help protect your personal information. Take some time to learn about the security and privacy settings in your browser. Some tools help you to control the amount of personal information you put online; others allow you to wipe the details of sites you have visited, or searches you have made, from your computer. Install antivirus and security software and keep this software updated.



# Social networking – privacy settings and what to post

---

People use social networking sites to keep in touch with friends and family, make new friends or business contacts, or share opinions. These sites allow you to share personal information, opinions and videos or photos. It is important to remember, however, that any information you post on a site could be public and may be seen by lots of people.

Most sites allow you to control how public or private your information is – these controls are usually called 'privacy settings'. While some sites set privacy settings automatically at their most 'private' level, on others all your information could be available to anyone unless you change the privacy setting. If you don't understand what a particular setting means in practice, don't post any information until you have found out.

Here are a few things you should consider before posting information or images on social networking sites:

- Find out how the privacy settings offered can limit access to your personal information.
  - Adjust your privacy settings so that information about your family and children is shared only with those you know well.
  - Don't include too much personal information that could make you vulnerable to identity fraud.
- Think carefully before posting information – would you want your employer or potential employer to see those compromising pictures?
  - Review your information regularly – what may have seemed like a good idea at the time may not seem such a good idea some months or years later.
  - Get people's consent before you upload their pictures or personal information.
  - Use strong passwords and logins to prevent your account being misused.

## Children – helping them stay safe online

---

Children use the internet regularly and may be involved in more online activity than their parents. Some children may have greater technical knowledge than their parents, but they may be unable to identify the risks of giving too much personal information online, and may be unable to spot 'scams' as readily as adults. So:

- Take the time to get involved in your children's internet use and teach them about online safety.
- Explain to children that they should not give any personal information online, e.g. full name, address, mobile number, email address, school name etc, if they would not want it freely available in the offline world.
- Explain that people online may be lying about who they are, and ensure your children know they must always get your permission before agreeing to meet anyone.
- Make children aware of spam or junk emails and explain that they should not open emails or texts from someone they don't know.

- If your children are using social networking sites, make sure they use appropriate privacy settings.
- Be aware that children may be accessing the internet via their games console or mobile phone.
- Consider using internet filtering and monitoring software for computers, mobiles or games consoles that your children own or use.

For more on child internet safety and useful materials aimed at children, parents and teachers, see:

<http://clickcleverclicksafe.direct.gov.uk/index.html>

<http://www.childnet-int.org/>

<http://www.thinkuknow.co.uk/>



# Your rights



You have the right to see information held about you online, and to get it corrected if it is wrong, in the same way as you do for information held in more traditional ways.

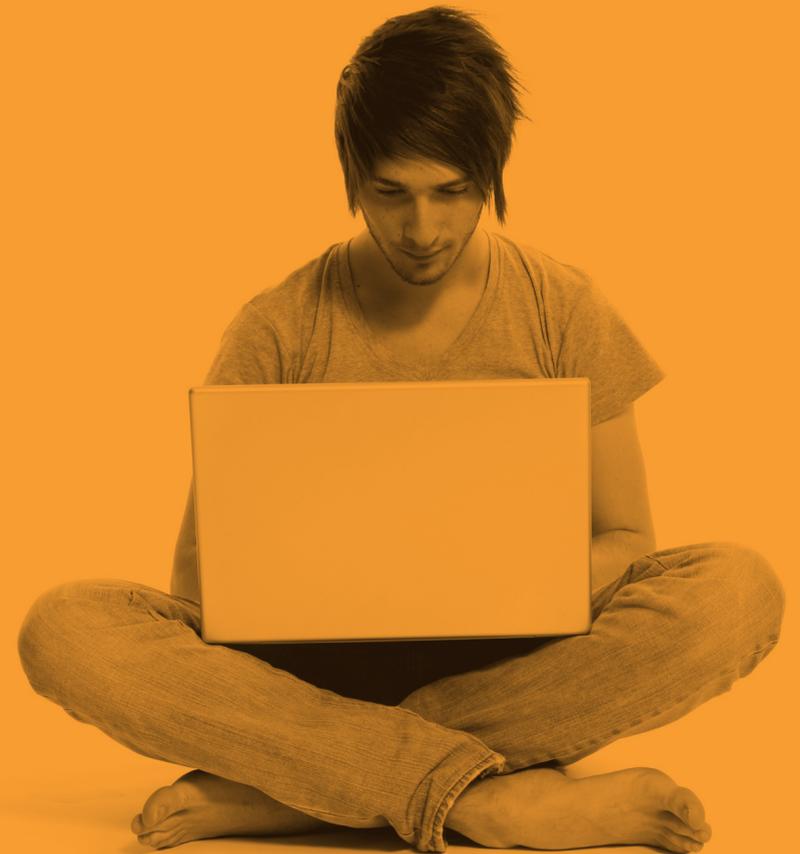
You also have the right to stop organisations using your information to send you direct marketing. You should get the opportunity to opt in or opt out of receiving such marketing at the point you give your personal details. You should also have the opportunity to change your preference later if you change your mind.

If you would like to see or correct personal information that is held about you, or if you think there is a problem with how your personal information has been collected online, or how it is being used, you should first contact the person or organisation responsible for collecting the information.

The provider of the service or website you gave the information to should give details of how you can contact those responsible – often this information is in the privacy notice on its website.

If you complain to an organisation about the collection or use of your personal information and are not satisfied with the response, you can complain to the Information Commissioner.

For more information about your rights and how to access your personal information, please visit the Information Commissioner's Office (ICO) website: <http://www.ico.gov.uk/> or contact our helpline on 0303 123 1113.



If you would like to contact us please call 0303 123 1113  
[www.ico.gov.uk](http://www.ico.gov.uk)  
Information Commissioner's Office,  
Wycliffe House, Water Lane,  
Wilmslow, Cheshire SK9 5AF

July 2010

**ico.**

Information Commissioner's Office

Upholding information rights