



## Data Protection Good Practice Note

### Collecting personal information using websites

**If you are interested in collecting personal information for marketing purposes, please see the separate guidance on the Privacy and Electronic Communications Regulations 2003 on our website (see note 1).**

#### **1 If we collect personal information directly from individuals through our website, what information should we give them and when?**

You must process personal information fairly, so website operators who collect personal information directly from individuals must always make sure that those individuals are aware of:

- the identity of the person or organisation responsible for operating the website and of anyone else who collects personal information through the site;
- what you will process their information for; and
- any other information needed to make sure the processing is fair to individuals, taking account of the specific circumstances of the processing. This will include telling individuals if you will disclose any information about them to third parties, including to other companies within the same group.

This information is often included as part of a privacy notice or statement. Your privacy notice should describe what you do and don't do with the personal information, as well as telling individuals about their rights and how to exercise them. For example, individuals have a right to be told if personal information about them is being processed, and to have a copy of this information. You should also tell them how to go about doing this. The privacy statement must include the physical address of the website operator, unless this is clearly available on the site.

Unless the use that you intend to make of the personal information is obvious, website operators must give this information to individuals before they collect any personal information from them.

Remember that people will not necessarily visit a website through its home page. They may access a particular page through a hyperlink. You should provide the above information at any point on the site where you collect personal information.

You also need to bear in mind that there may be more than one person or organisation involved in collecting personal information through the site, particularly if a third party places banner advertising or provides a secure payment system. In these cases, you should identify all those collecting personal information.

You may want to use the Information Commissioner's padlock symbol. This is intended to alert individuals to the fact that their information is being collected and draws their attention to the explanation of how it will be used.

## **2 We have a privacy statement on our website - is this enough?**

No, it is not enough simply to say 'click here to see our privacy statement'. You need to show some basic description of your use of individual's information wherever personal information is collected, even when more detailed information is provided elsewhere.

ICO research has shown that a layered notice is the most effective at making individuals aware of how you will use their information. This usually consists of three linked notices which are increasingly concise. The longest one will be the full notice and should include all legal provisions. The condensed notice contains the main information, usually organised under subheadings. The short notice merely draws attention to how personal information will be used in the broadest terms and is used where there is not enough space for the other layers, so will not usually apply to websites. The notice should be clear and easy to read and understand, and placed wherever personal information is collected.

You can get help designing a privacy statement from the Organisation for Economic Co-operation and Development (OECD) website which has a privacy policy generator (see note 2). Guidance on how to assess your current privacy notice and create layered notices has been produced by the Centre for Information Policy Leadership in their document 'Ten steps to develop a multilayered privacy notice' (see note 3).

## **3 What are the implications if we use 'cookies' to build up profiles of visitors to our site?**

Website operators using cookies are able to track the on-line movements of an individual and may be used to develop a profile of them. If the operator intends to link this profile to a name and postal address, or an e-mail address, this is personal information covered by the Data Protection Act 1998 (the Act). However, operators can develop and use profiles by using cookies without collecting traditional identifiers. Our view is that, in the context of the on-line world, the information that identifies an individual is that which uniquely locates them in the world, by distinguishing them from others. So, profiles based on the information collected by cookies which are linked to other information which uniquely identifies the individual are personal information and covered by the Act.

Websites use cookies in a variety of ways. They are not always used to develop profiles of individuals but, under Regulation 6 of the Privacy and Electronic Communication Regulations 2003, you must tell visitors to your site wherever a cookie or other tracking system collects information, and you must give them the opportunity to refuse their continued use. You could do this with a notice before you collect the information, or in the privacy statement. However, if you choose to let

---

Note 2 [www.oecd.org/document/39/0,2340,en\\_2649\\_37441\\_28863271\\_1\\_1\\_1\\_37441,00.html](http://www.oecd.org/document/39/0,2340,en_2649_37441_28863271_1_1_1_37441,00.html)

Note 3 [www.hunton.com/files/tbl\\_s47Details/FileUpload265/1405/Ten\\_Steps\\_whitepaper.pdf](http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf)

people know through the privacy statement, it is important to have some reference to the use of tracking technology clearly displayed to all visitors.

The website [www.allaboutcookies.org](http://www.allaboutcookies.org) is a useful source of information.

#### **4 Is the position the same if we use IP addresses to profile our site visitors?**

In theory, yes. In practice, it is difficult to use IP addresses to build up personalised profiles. Many IP addresses, particularly those allocated to individuals, are 'dynamic'. This means that each time a user connects to their internet service provider (ISP), they are given an IP address, and this will be different each time. So if it is only the ISP who can link the IP address to an individual it is difficult to see how the Act can cover collecting dynamic IP addresses without any other identifying or distinguishing information.

Some IP addresses are 'static', and these are different. Like some cookies, they can be linked to a particular computer which may then be linked to an individual user. Where a link is established and profiles are created based on static IP addresses, the addresses and the profiles would be personal information and covered by the Act. However, it is not easy to distinguish between dynamic and static IP addresses, so there is limited scope for using them for personalised profiling.

#### **5 We've been told we can use a web-bug to collect information about visitors to our site. What is a web-bug and can using one comply with the Act?**

A web-bug is usually a small graphics file, usually only 1 x 1 pixel in size, that is designed to monitor the time, type of web browser being used and IP address of a computer when accessing a web page or viewing an e-mail message. Like cookies, using this device may result in you processing personal information. The Act does not generally stop you using these devices. However, if the device is invisible to the person it is monitoring, it is difficult to see how you can collect that person's information fairly without telling them that monitoring is taking place, who is doing it and why.

Under regulation 6 of the Privacy and Electronic Communication Regulations 2003, you must tell visitors to your site wherever a cookie or other tracking system collects information and you must give them the opportunity to refuse their continued use. You could do this with a notice before you collect the information, or in the privacy statement. However, if you choose to let people know through the privacy statement, it is important to have some reference to the use of tracking technology clearly displayed to all visitors.

#### **6 Are we allowed to use personal information available on the internet for our own purposes?**

You should be careful when getting personal information from a source other than the individual. Using this personal information will usually be covered by the Act.

If an individual puts their e-mail address in the public domain, for example, in a chat room, this does not mean you can use this for any purpose you see fit. If you use 'spiders' or other scavenging-type programmes to collect e-mail addresses, or other

personal information from the internet, you are likely to breach the Act unless you are then using the information for the same reasons as it was provided for originally.

Individuals may choose to put personal information on the internet, for example, by putting their CV on their own website. They should be wary of doing this, as it leaves the information open to misuse. However, this does not remove your responsibility to make sure you only use the information fairly, for the purpose (whether express or implied) it was posted on the internet.

## **7 If we have collected information about someone other than directly from them, do we have to tell them we have it?**

If you get information from a third party, for example, directly from another website operator or harvested from a website, you still have a duty to make sure any subsequent processing of the information is fair. This may involve making sure that the individual knows that you hold their information and what you are using it for.

In some cases, it may be possible for you to tell individuals before you collect their information from a third party that you will get information about them indirectly, and what you will use it for. For example, when an individual registers with your website and you have already told them in your notice that you will be getting information from other sources.

In other cases, the source of the information may have already explained to the individual, at the point at which they collected the information, that you will also collect and use that information. For example, where website operators routinely exchange information and their fair processing notices explain this.

If individuals do not have the necessary information to make the processing of their personal information fair, you should provide it as soon as possible after obtaining their personal information. If you intend to disclose information, you should tell individuals no later than the time you first disclose it.

You do not have to contact the individual if this would involve 'disproportionate effort'. If you think this is the case, you will have to make sure you document your decision and can explain this to anyone who asks. You should be aware that as you can provide information to individuals easily on-line, for example, by sending automated e-mails, there are very limited circumstances in which you can rely on this exemption.

## **8 Our website is directed at children. Are there any special rules we have to follow?**

Websites that collect information from children must have stronger safeguards in place to make sure any processing is fair. You should recognise that children generally have a lower level of understanding than adults, and so notices explaining the way you will use their information should be appropriate to their level, and should not exploit any lack of understanding. The language of the explanation should be clear and appropriate to the age group the website is aimed at. If you ask a child to provide personal information you need consent from a parent or guardian, unless it is reasonable to believe the child clearly understands what is involved and they are capable of making an informed decision.

The Act does not state a precise age at which a child can act in their own right. It depends on the capacity of the child and how complicated the proposition being put to them is. As a general rule, we consider the standard adopted by TrustUK ([www.trustuk.org.uk](http://www.trustuk.org.uk)) to be reasonable:

'TrustUK approved webtraders recognise children need to be treated differently from adults. They will not market their products in any way that exploits children, nor will they collect information from children under 12 without first obtaining the permission of a parent or guardian. They will not collect personal data about adults from children.' (see note 4)

The above standard is based on a definition of a child as a person aged 16 or under.

There are certain practices that are likely to breach the Act, for example, collecting information about other people from children, and enticing children to reveal information to win a prize or similar. If you are going to disclose or transfer personal information collected from children to third parties, you need to have the explicit and verifiable consent of the child's parent or guardian, unless you can be sure that the child really appreciates what is going on and the consequences of their actions.

If you want to publish a child's personal information on the internet, you should usually get the verifiable consent of the child's parent or guardian. Whether you need the parents' or guardians' consent for the publication, or that of the child, will depend on the circumstances, in particular, the child's age and whether you can be sure the child fully understands the implications of making their information available on the internet.

If you need parental consent, you must have some way of verifying this. It will not usually be enough to ask children to confirm their parents have agreed by using a mouse click. If you need parental consent but decide that verifying the consent will involve disproportionate effort, you should not carry out your proposed activity.

## **9 We collect personal information through our website. Do we have to use an encryption-based transmission system?**

You are responsible for processing personal information securely. You must adopt appropriate technical and organisational measures to protect the information you collect. It is difficult to see how you could do this without having a secure, encryption-based transmission system if the personal information is sensitive or poses a risk to individuals, for example, if it includes credit card numbers.

You should be aware that although a secure transmission system will protect the personal information in transit, there is a potentially greater threat to the security of the information when it is decrypted and held on a website operator's server. Any sensitive personal information, or information that would pose a risk to individuals, should not be held on a website server unless it is properly secured by encryption or similar techniques.

## **10 If we use another company to host our website, who is responsible for data protection?**

The 'data controller' is responsible for complying with the Data Protection Act 1998. This is the company or person who determines how and why the personal information is processed. The data controller does not have to own the processing equipment. If you employ a specialist company to host a website on your behalf you will be the data controller for the information collected or disclosed through that website. Where a data controller employs another company to host or operate their website they must have a written contract which requires that:

- the processor must only act on the data controller's instructions; and
- there must be appropriate technical and organisational security measures in place.

The ICO have produced a good practice note for businesses wanting to outsource processing to other companies (see note 5).

## **11 Can we publish personal information on our website?**

Putting personal information on a website will often result in transfers to countries outside the UK. The transfers will take place when the website is accessed by someone outside the UK. If you load information onto a server based in the UK so that it can be accessed through a website you should consider the potential for a transfer to take place and whether that would be fair for the individuals involved given the potential effect on them. The ICO have produced guidance on international transfers (see note 6).

In some cases, the risks from a transfer may be negligible. For example, publishing details of sporting achievements of well-known athletes. It may also be relevant if the individual cannot be contacted through the information published, although you will need to take account of the sensitivity of any information.

In other cases, it may be necessary to get the individual's informed and freely given consent. This means you need to explain the possible consequences of publishing the information, that the individual does not face a penalty for declining and can withdraw their consent at any time.

In most cases, you will need to consider the fairness of the processing. For example, a sports club may have traditionally published member names and contact details in a handbook distributed to all members and local libraries. The club now wants to publish this information on its website. Although the information has always been publicly available, the implications for members are now significantly different. Fairness means that individuals should be told their details are going to be published on a website and those who object should have their wishes respected. If the information is only going to be available to club members, the club should use technical measures to prevent access by unauthorised individuals, such as by preventing general access to the site or that part of the site, by using a password.

---

Note 5 [www.ico.gov.uk](http://www.ico.gov.uk) - Outsourcing - a guide for small and medium sized businesses

Note 6 [www.ico.gov.uk](http://www.ico.gov.uk) - General advice on how to comply with the 8th data protection principle

## **12 If we want to use the personal information we have collected through our website for a different purpose, can we simply change our privacy statement?**

No. If you change the privacy statement, it will only affect how you use any information collected after the date of the change. Visitors who provided information before the change will have done so in light of the previous privacy statement, so you must honour the assurances you gave them.

The safest way to change your use of personal information is to get the individuals' consent. In other words, you must explain your proposed new use of their information and only proceed when they have indicated positively that they agree. This is sometimes referred to as an 'opt-in' for individuals. Not responding to an e-mail message does not mean they are giving consent

This approach will be necessary if you or others want to use the information for a new purpose, or disclose to different organisations than are mentioned in your privacy statement. It will also be necessary if the information is sensitive, or subject to a duty of confidentiality that the new use would breach.

In some cases, it will be enough to advise the individuals of the new use and give them an opportunity to object. This will be the case if the new use is not for a new purpose, or the nature and purpose of the disclosure is close to the terms in your privacy statement. For example, if your site was originally set up to sell books, and now you want to sell cds and market them to individuals. Originally, you told your customers you would only use their information for marketing, and gave them an opportunity to opt out. Without any other information, they would have assumed the marketing was limited to books. Marketing cds is close to but outside the terms of your privacy statement, so you should tell your customers who consented to marketing about this new use of their information and give them another opportunity to opt out - either from all marketing, or from marketing cds. You should not contact the customers who originally opted out.

In other cases, the new use might be within the original privacy statement. For example, if it referred to marketing a range of products, even if at the time this was limited to books. If it now includes marketing cds, you don't need to advise your customers specifically about this, as the products are closely related. However, you should respect the wishes of any customer who then objects to the new marketing.

If the new products are substantially different, for example, if they now include financial services, your customers would not expect this kind of marketing, even if you could argue that your privacy statement may have covered it. What is important is the customers' expectations of what you will use their information for. Depending on how much the new use differs from their reasonable expectations, customers should opt in rather than opt out.



If you are not established in the EEA in some circumstances you might be subject to the UK Act, for example, if you use equipment in the UK to process the information. This may be the case where you put cookies on the computers of UK internet users to create a profile of their on-line behaviour, if your site is hosted in the UK, or you use another organisation in the UK to process the information collected through the site.

If you are established in the UK but choose to host your site outside the EEA, the UK Act will still apply to your collection and further use of information.

## **16 What about if I only use my website for personal use?**

If you only process personal information for your family or household affairs, including recreational purposes, you do not need to notify and you are exempt from the principles in the Act. However, the Information Commissioner is still able to use his investigation and enforcement powers to determine whether the exemption applies, for example, if you also use your site for business purposes.

**We may update these frequently asked questions in light of legal, technological or other developments. Please let us know if there are any questions of general interest to website operators that we have not covered.**

### **More information**

If you need any more information about this or any other aspect of data protection, please contact us.

Phone: 08456 30 60 60  
01625 54 57 45

E-mail: please use the online enquiry form on our website

Website: [www.ico.gov.uk](http://www.ico.gov.uk)