

INFORMATION SECURITY: PRIVACY POLICY CHECKLIST

[The information you collect](#)
[Why you collect the information](#)
[How you handle the information](#)
[Changing personal information](#)
[Policy changes](#)
[Contact information](#)
[Children](#)
[Further help and advice](#)

If you collect data or information about your web site users (who are normally your customers), you should publish a prominent, readily accessible statement on your web site regarding the manner in which you collect and use their personal data.

This is often referred to as a 'Privacy Policy'. Please note that this is in addition to the legal requirement to register your use of personal data with the Office of the Information Commissioner under the Data Protection Act (see www.ico.gov.uk). A Privacy Policy helps build trust between you and your customers. The following checklist provides steps that, if taken and adhered to, will assure your customers of your commitment to their privacy. A Privacy Policy should include clauses covering the following:

The information you collect

This section covers the type of information collected about people as they visit your web site. It normally includes a statement on consent. An example of such a statement might be:

'By submitting personal data manually or in electronic form to this web site, or by using this site, you give your consent that all personal data you submit may be processed in the manner and for the purposes described below.'

The section should also include specifics about the type of information gathered. The following wordings are examples of such statements:

'If you do nothing other than read pages or download information while using this web site, we will capture and store information about your visit. This information will not identify you; it relates to:

- the Internet domain (e.g. www.company.co.uk) and IP address from which you access the web site
- the type of browser (Internet Explorer or Netscape) and operating system (Windows, UNIX) you use
- the date and time of your visit
- the pages you visit
- the address of the web site from which you linked to us (if applicable).

We use this information to make each visit more rewarding, and to provide us with information to help improve our service. We do not know (and do not want to know) the identities of people who visit us in this way.'

If you collect information offered freely by users (such as user e-mail addresses), you must state your reasons for doing so.

If you use automated techniques of collecting data, you should state how this is done. If you use cookies, you should inform readers and offer them the option of rejecting these. You might also provide a brief description of cookies: 'A cookie is a piece of information sent via your Internet browser and stored on your local hard drive. Some of them are deleted when you shut down your browser; others are stored for longer. Cookies do no harm in themselves, but you can choose to accept or reject them by changing the settings on your browser.'

Why you collect the information

This section aims to inform (and assure) your customers of the reasons for collecting information. These may vary, but will mainly include:

- improving customer service
- giving better access to products/services of interest
- providing customers with product updates, offers and announcements.

If you intend to carry out market research using such data, you should say so in your Privacy Policy. It is important to state that you manage all collected data in accordance with the Data Protection Act (see www.ico.gov.uk).

How you handle the information

As stated above, it is essential that you manage the personal data you receive in accordance with the Data Protection Act. Let your readers know that this is your policy. You should also ensure they are aware that under the Act they are entitled to access information about them, and that they have the right to demand that this information is amended and/or deleted should it not comply with the Act's principles. You should provide contact details to facilitate this access and amendment.

Some Privacy Policies provide detail on how data, such as passwords, Internet firewalls and employee training, are protected. You may wish to include such information, particularly if you handle sensitive personal information.

Information disclosure is an important aspect of the Data Protection Act and you should state clearly the circumstances under which you disclose data to third parties. Such circumstances might include the disclosure of data:

- To companies acting for you in performing your normal business, e.g. a mailing company that sends out customer mail shots.
- When obliged to do so by law. This would include police investigations.
- When protecting customer interests, such as legal liability.
- In unusual circumstances, such as a company merger.

You must include an option to opt out of services such as e-mail shots. Provide e-mail and telephone contact details to facilitate this.

Changing personal information – remind people of their right of subject access

You should provide a facility for your site visitors to view or change personal information about themselves. Make sure you can authenticate individuals who seek to do so, and ensure they are reminded of their rights under the Data Protection Act. Provide appropriate contact details.

Policy changes

Make sure you publish changes to your Privacy Policy in a timely manner and that readers are informed of these amendments. This section should include a statement as follows:

'The personal information we collect and maintain will be subject to the version of the Privacy Policy in effect at the time of collection. We reserve the right to change the Privacy Policy from time to time and will provide notice of these changes on the home page of our web site. You should make sure you periodically review the Privacy Policy to make sure it meets your needs.'

Contact information

Provide contact details for your site visitors, including information about:

- webmaster
- information change
- complaints
- data protection queries

It is possible that a single person may perform all these roles. Make sure you provide e-mail, telephone and postal address details.

Children

If your site is not intended for children, it is worth saying so. The following words provide a template:

'This web site is not intended for children under 13 years of age. We neither knowingly solicit nor collect personal information from or about children, nor do we knowingly market our products or services to them.'

THE INFORMATION PROVIDED HERE IS TO BE TREATED AS GUIDANCE ONLY. IT IS NOT INTENDED TO REPLACE PROFESSIONAL LEGAL OPINION.

Please refer to the [Legislation](#) section in our business advice pages (see below) for further information.

Further help and advice

General

BERR Information Security Health Check Tool
<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page
www.berr.gov.uk/sectors/infosec

BERR Information Security Business Advice pages
<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)
<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>