

Data Protection Act



Your responsibilities and obligations to data protection

If you handle personal information about individuals, you have a number of legal obligations to protect that information under the Data Protection Act 1998.

What security measures should I take to protect the personal data I hold?



Top tips on how to protect the personal data you hold.

For computer security:

- Install a firewall and virus-checking on your computers.
- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow your staff access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

For using emails securely:

- Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.

- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

For using faxes securely:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

For other security:

- Shred all your confidential paper waste.
- Check the physical security of your premises.
- Train your staff:
 - so they know what is expected of them;
 - to be wary of people who may try to trick them into giving out personal details;
 - so that they can be prosecuted if they deliberately give out personal details without permission;
- to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
- not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

You can find more information about data security on our topic page titled [Our approach to encryption](#). For further guidance please read [Security of personal information](#).

For a good source of advice in plain English on security go to the government and business sponsored website getsafeonline.org.

What should I do if I lose personal data?



If, despite the security measures you take to protect the personal data you hold, a breach of security occurs, it is important to deal with the breach effectively. The breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. However the breach occurs, you must respond to and manage the incident appropriately. You will need a strategy for dealing with the breach, including:

- a recovery plan, including damage limitation;
- assessing the risks associated with the breach;
- informing the appropriate people and organisations that the breach has occurred; and
- reviewing your response and updating your information security.

Read more about [how to respond to a security breach](#) and our more detailed guidance.

Use our [Security breach notification form](#) to report a breach to us.