Personal data security: how to prevent some common personal data breaches

1. How to disclose information safely

Check documents, including spreadsheets, for hidden personal information and remove or redact it, where appropriate. This will minimise the risk of an accidental breach of personal information when disclosing documents online or sending them to the public. See our guidance on How to disclose information safely for more information.

2. Disable autofill in your email settings

If people's email addresses come up automatically when starting a new email message then you have autofill enabled in your settings. This tool may save time, but it puts you more at risk of sending an email to the wrong person, especially if email addresses are similar.

3. Using the blind carbon copy function

Disclosing email addresses can reveal people's information and potentially cause significant harm. To protect the personal information you hold, you should assess your methods for sending bulk mailing. For more information, please see our guidance on sending bulk communications.

4. Send electronic documents securely

If you need to send electronic documents, consider encrypting or password-protecting them, especially if what you're sending contains sensitive information. This reduces the risk of the wrong person being able to access the documents. You could also consider using a secure email service or a portal. When sharing the password with a recipient consider providing this via an alternative method, such as telling them over the phone or sending it via text.

5. Keep your IT systems up-to-date and be vigilant to cyber security threats

You can reduce your risk of cyber threats, such as attacks on computer systems, by making sure you regularly install security updates. Cyber attacks can also affect organisations of any size and in any sector. The guidance issued by the National Cyber Security Centre (NCSC) can help you to prepare for and deal with cyber security incidents you may experience. You can find out more through the NCSC website.

6. Only access or use data with permission

Training is a key way to ensure people are aware of their responsibilities around accessing and using personal data. This includes not accessing or using data without permission and not disclosing data to unauthorised parties. Access to personal data should also be controlled through managing access permissions.

7. Double-check your outgoing post

From putting a letter in the wrong envelope to using the wrong address, it's easy to send post to the wrong person. Ensure you double check any post you are sending. You should check what's included and who it's going to. You should also consider if there is a safer way to send personal data, such as using secure email.

8. Reduce paperwork where possible

Paperwork can be easily lost or fall into the wrong hands when left in an unsecure location. Where possible, use secure electronic storage to reduce the amount of printed paperwork. This also includes scanning documents, storing them electronically and then disposing of paperwork safely. Take care if you're removing paperwork from an office and ensure this is handled securely when in transit.

9. Be careful when disclosing personal data

When responding to requests for information you should ensure you redact any personal data that should not be included. There should be clear and accessible written procedures in place on redacting information, which include robust checking measures. You should also ensure that appropriate redaction software is used to reduce the risk of personal data being shared with the wrong person.

10. Secure the data on electronic devices

We carry a lot of personal data on electronic devices, often without realising. Make sure you're prepared in case a device is lost or stolen. Review the security measures in place on devices and ensure they are password protected and encrypted. You could implement multi-factor authentication or the ability to wipe the contents of the device remotely.