HM Government

SHARE WITH CARE

How to minimise the risk of a data breach

It might not be possible to prevent every data breach, but here are some steps that everyone can take to reduce the risk.

1. Name your documents correctly and clearly

All departments should have a naming convention. If you name your documents using the same format every time, it makes it easier to find the right one. It's also less likely that someone will attach the wrong document to an email. Ensure not to include sensitive information in document titles.

2. Use blank template documents and store them separately

If you use template documents, make sure you create a new copy of it every time and avoid overwriting a previous document. Blank templates should be stored away from pre-populated ones to avoid someone seeing this information by mistake.

3. Store sensitive information securely

It is everybody's responsibility to keep sensitive information safe and make sure no-one has access to it without authorisation. Some simple security measures could include using the correct Classification and Handling markers, and using strong passwords on all your devices. If you handle sensitive information, you must take extra steps to protect it from getting lost, damaged or stolen. You also must make sure no-one accesses or alters it without permission.

4. Take care when redacting data

When responding to a request for information, you'll often need to send copies of data. You may need to remove or redact sensitive information which isn't relevant to the request, such information about other people. When doing this, be thorough and check the information can't still be seen or recovered.

5. Take care when talking to others

Be careful not to talk about personal or sensitive matters where you can be overheard or overseen, or tell a person something they're not entitled to know.

HM Government

SHARE WITH CARE

6. Share information safely

Some actions you can take to ensure you are sharing information safely include checking for hidden data in attachments, checking the recipients are correct and that they are authorised to receive the information, and when emailing multiple recipients, use bulk email services, mail merge, or secure data transfer services where available (If these are unavailable, BCC should be used).

7. Review your access controls

Not everyone needs access to everything, so if you are a manager think about whether you can tighten access controls by only allowing your staff to have access to data that they need to carry out their role, and remove any access that they don't need.

8. Adhere to the Clear Desk Policy and Remote Working Policy

Ensure you do not store paperwork on your desk or workspace, including folders, cards, and Post-it notes that could expose sensitive information. This applies both in the office and while you're working from home. You should familiarise yourself with the Remote Working Policy which details how you should handle sensitive information when working away from the office.

9. Reporting incidents

We understand that accidents can happen. It is important that you understand your local reporting procedures because reporting incidents early can prevent harm.