



What to do when things go wrong: how to respond to a data breach

A data breach is the unauthorised exposure, disclosure, or loss of sensitive information. If you think you've spotted a data breach, whether accidental or deliberate, and you're worried about what to do next, we can help. This guide has three simple steps that you should take after discovering a data breach.

Step one: Don't panic

It's understandable if you're concerned about what happens next, but we are here to support you, and our aim is to provide advice to avoid similar incidents in the future.

Step two: Act quickly

If you can recover the data, do so immediately;

- If the sensitive data was sent by email, try to recall the email as soon as possible and if you can't recall it, contact the person who received it and ask them to delete it.
- If you had the sensitive data in physical format and you don't know where you've lost it, retrace your steps. If you think it's been lost in an office or building, you could try contacting reception.

Step three: Take action

As soon as you discover a data breach, you must contact your line manager and your local security team as soon as possible. They will investigate and advise on what steps to take next. If the data breach meets the threshold, your security team will report it to the Information Commissioner's Office (ICO).

Data protection legislation says it is mandatory for organisations to report a data breach to the ICO without undue delay and within 72 hours unless we are certain it is unlikely to cause risk to people's rights and freedoms. This is why it is very important that you report data breaches as soon as you find out about them.

Top tip

When you report the incident to your local security team, try to provide as much information as possible. Give as detailed a description as you can about what happened and why.

SOME THINGS YOU CAN'T UNDO