Three Counties Data Protection

Data Breach Response Guide

A practical guide for small businesses, charities and community organisations

First things first: don't panic

A "data breach" sounds serious, but it simply means personal information has been:

- sent to the wrong person
- lost or deleted
- accessed without permission
- shared when it shouldn't have been

Not all breaches need to be reported to the ICO - but all of them should be assessed.

The key is: act quickly, calmly, and consistently.

Step 1. Contain the breach

Stop the problem getting worse.

Ask:

- Can the email be recalled or deleted?
- Can access be removed (e.g. shared folder, system login)?
- Has anything been posted publicly that can be taken down?
- Do passwords need changing?

If it involves paper:

- retrieve documents if possible
- secure anything left out or accessible

Step 2. Record what happened

Write it down straight away while it's fresh.

Include:

- what happened (plain English, no jargon needed)
- when it happened
- what type of information was involved
- how many people are affected (if known)
- who discovered it and when

Tip: an email to yourself or a simple note is fine if you don't have a formal log.

Step 3. Assess The Risk

This determines what happens next.

Ask three simple questions:

1. What type of information is involved?

Higher risk includes:

- health information
- financial details
- IDs (passport, NI numbers)
- safeguarding information
- children's data

2. How serious could the impact be?

Could it cause:

- distress or embarrassment?
- financial harm?
- identity fraud?
- risk to safety or safeguarding?

3. How many people are affected?

Step 4. Decide if It needs to be reported to the ICO

*In the UK, you must report a breach to the Information Commissioner's Office (ICO) if it is **likely to result in a risk to people's rights and freedoms**.*

You usually do **NOT** need to report if:

- the information is low risk (e.g. basic contact details only)
- it was quickly contained
- no real harm is likely

You usually **DO** need to report if:

- sensitive or financial data is involved
- children's or vulnerable people's data is involved
- data has been exposed publicly or widely
- there is a real risk of harm or fraud

If in doubt, it's usually safer to assess it formally.

You can report here: https://ico.org.uk/for-organisations/report-a-breach/

Step 5. Tell the affected people (if needed)

*You must inform individuals if the breach is likely to result in **high risk to them**.*

This might include:

- explaining what happened
- what data was involved
- what you are doing about it
- what they should do (e.g. change passwords, be alert for scams)

Keep it:

- clear
- factual
- not defensive

6. Take action to prevent it happening again

Once things are under control, ask:

- How did this happen?
- What could stop it happening again?

Common fixes include:

- staff training
- password changes / MFA
- tighter access controls
- better procedures for emailing or file sharing
- clearer roles and responsibilities

Step 7. Record your decision

Even if you don't report it, you should document:

- your assessment
- your decision
- why you made it

This is important for accountability under UK GDPR.

If you're unsure what to do

A good rule of thumb:

If you're thinking "this doesn't feel quite right", treat it as a breach and assess it properly.

You can seek external advice before making a final decision - but don't delay urgent containment steps.

Final reminder

Most breaches are caused by simple human error - not negligence. What matters is:

- how quickly you act
- whether you contain the issue
- and what you learn from it

hello@threecountiesdata.co.uk • www.threecountiesdata.co.uk

Three Counties Data Protection

Practical data protection support for small businesses, charities and community organisations across Worcestershire, Herefordshire and Gloucestershire.