Personal data breach: what to do

All staff | Tasks for the DPO | Guidance on this procedure

Found or caused a data breach? Immediately notify our data protection officer (DPO)

Our DPO is:

Telephone: **Email:**

The DPO will ...

Alert the headteacher and chair of governors

Contain and minimise the impact of the breach

Taking all reasonable efforts, and assisted by relevant staff where necessary

Assess the potential consequences

How serious are they? How likely are they to happen?

Risk to someone's rights and freedoms: is it *likely*?

Could the breach put someone at risk of discrimination, identity theft, damage or disadvantage?

NO → Risk to someone's rights and freedoms: is it *high*?

YES

Report the breach to the ICO within 72 hours

Go to **www.ico.org.uk/for-organisations/report-a-breach/** or call **0303 123 1113**.

Provide information on:

- The nature of the breach, including where possible: the categories and approximate number of individuals concerned, the categories and approximate number of data records concerned
- The likely consequences of the breach
- The measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on those concerned

Give a point of contact – usually the DPO.

If not all details are available, report as much as possible and explain that there is a delay, the reasons why, and when you'll have further information. Submit the remaining information ASAP.

Risk to someone's rights and freedoms: is it *high*?

How serious are the risks? How likely are they to happen?

NO → Review and record the breach

YES

Inform the affected individual(s) promptly

Do this in writing and set out:

- Your (the DPO's) name and contact details
- The likely consequences of the breach
- The measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on individuals

Notify any third parties who can mitigate the impact of the breach

For example, the police, insurers, banks or credit card companies

What is a data breach?

It's a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A breach might involve:

- Non-anonymised data being published on the school website showing test results of children eligible for the pupil premium
- Safeguarding information about a child being made available to unauthorised people
- The theft of a school laptop containing non-encrypted personal data about pupils

Why must you escalate a data breach?

1. If someone's personal data falls into the wrong hands it can result in serious harm to that person
2. We are legally required to investigate data breaches
3. Learning what went wrong will help us to adapt procedures and prevent future breaches

Review and record the breach

Discuss with the headteacher:

- What happened
- How we can stop it from happening again
- Whether a process or system regularly has minor incidents

Record:

- Facts and cause
- Effects
- All decisions taken – including whether or not to report to the ICO/individuals affected
- Action taken to contain the breach and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all data breaches are stored here:

This procedure is based on guidance from the Information Commissioner's Office, the body responsible for upholding information rights in the UK