



Personal Data Breach Procedures

Date written / reviewed	March 2025
Date of next review	March 2028
Headteacher	<i>R Swaby</i>
Chair of Governors	<i>M Hopkins</i>

This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the HEADTEACHER / HEADTEACHER / DPO.
- The HEADTEACHER / HEADTEACHER / DPO will investigate the report and determine whether a breach has occurred. To decide, the HEADTEACHER / HEADTEACHER / DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The HEADTEACHER / HEADTEACHER / DPO will alert the Headteacher and the chair of Governors.
- The HEADTEACHER / HEADTEACHER / DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The HEADTEACHER / HEADTEACHER / DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The HEADTEACHER / HEADTEACHER / DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the HEADTEACHER / HEADTEACHER / DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the HEADTEACHER / DPO must notify the ICO.

- The HEADTEACHER / DPO will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on an encrypted software and kept in a locked cupboard / room.
- Where the ICO must be notified, the HEADTEACHER / DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the HEADTEACHER / DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the HEADTEACHER / DPO.
 - A description of the likely consequences of the personal data breach.

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the HEADTEACHER / DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the HEADTEACHER / DPO expects to have further information. The HEADTEACHER / DPO will submit the remaining information as soon as possible.
- The HEADTEACHER / DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the HEADTEACHER / DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the HEADTEACHER / DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The HEADTEACHER / DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The HEADTEACHER / DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on an encrypted hard drive and locked in the Headteacher's office.
- The HEADTEACHER / DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

Follow the guidance set out in appendix 1

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the HEADTEACHER / DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the HEADTEACHER / DPO will ask the IT department to recall it.
- In any cases where the recall is unsuccessful, the HEADTEACHER / DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The HEADTEACHER / DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The HEADTEACHER / DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's cashless payment provider being hacked and parents' financial details stolen.

Personal data breach: what to do

All Staff

Tasks of the HEADTEACHER / DPO and

Guidance on this procedure

Found or caused a data breach? Immediately notify the Headteacher who will then notify the data protection office

Our HEADTEACHER / DPO is: Mr J Smith Oldham LA

Telephone: 0161 770 7600

Email: info@delph.oldham.sch.uk

The HEADTEACHER / DPO and

Alert the Headteacher (if incident reported directly to HEADTEACHER / DPO) and Chair

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 they are? 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?

Yes

Report the breach to the ICO within 72 hours

Go to www.ico.org.uk/for-organisation/reports-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 HEADTEACHER / DPO.

If not all the 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

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

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

Yes

Inform the affected individual(s) promptly

Do this in writing and set out:

- * Your (the HEADTEACHER / 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 on the breach

For example, the police, insurers, banks

What is a data breach?

It's a breach of security which leads to the accidental or unlawful destruction, loss alteration, unauthorized 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 it to the ICO/individuals affected
 - * Action taken to contain the breach and ensure it does not happen again (such as establishing a more robust process or training)
- Records of all data breaches are stored electronically on encrypted software in the HT office.