



## Appendix 1: Personal data breach procedure

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, trustee, or data processor must immediately notify the data protection compliance officer (DPCO) by, filling out an online reporting form on the GDPR portal
- The DPCO will investigate the report and determine whether a breach has occurred. To decide, the DPCO 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 unauthorized people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is likely that is the case, the DPCO will alert the headteacher and the chair of trustees
- The DPCO will make all reasonable efforts to contain and minimize the breach's impact. Relevant staff members or data processors should help the DPCO with this where necessary, and the DPCO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPCO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPCO will work out whether the breach must be reported to the ICO, and the individuals affected using the ICO's [self-assessment tool](#)
- The DPCO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPCO and the school on the school's computer system.
- Where the ICO must be notified, the DPCO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPCO 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 DPCO
  - A description of the 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 DPCO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPCO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPCO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPCO
  - A description of the 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 DPCO will consider, considering the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPCO 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 the school's computer system, or on a designated software solution

- The DPCO 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
- The DPCO and headteacher will meet termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

### **Actions to minimise the impact of data breaches**

We set out below the steps we might take to try and mitigate the impact of several types of data breach if they were to occur, 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 unauthorized 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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorized 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 DPCO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPCO 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
- **If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners**

Other types of breach that you might want to consider could include:

- Non-anonymised pupil exam results or staff pay information being shared with trustees.
- 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.
- Hardcopy reports sent to the wrong pupils or families.