# Personal data breach procedure

This procedure is based on [guidance on personal data breaches](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) produced by the ICO and will be used for any data breaches identified in the Trust or their schools.

**What is a personal data breach?**

‘A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.’ – ***Taken from the ICO Guide to GDPR***

On finding or causing a breach, or potential breach, the staff member, trustee/governor or data processor must immediately notify the DPO (ideally within 24 hours of the breach occurring).

The following steps will be followed:

1. On receipt of the notification, the DPO will inform the Governance Manager about the breach who will notify CEO and Chair of the Board.
2. The DPO will investigate the potential breach, and determine whether a breach has occurred. To decide, the 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

1. The 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)
2. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
3. The DPO will assess and recommend whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the 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 DPO must notify the ICO. Where the ICO must be notified, the DPO will do this via the [‘report a breach’ page of the ICO website](https://ico.org.uk/for-organisations/report-a-breach/) within 72 hours.

**Please note:** The Trust will prioritise the investigation and provide adequate resources as required.

1. The DPO instigates an investigation and produces a report on the breach (whether or not reported to the ICO). The report includes:

* how it happened and extent of the breach
* whether it could have been prevented.
* Academy measures taken immediately to mitigate the risk to the individuals
* The risks to the data subjects (individuals) because of the breach:
* Any security measures in place that will protect the information:
* Required actions and development areas following the personal data breach to prevent re-occurrence

1. The 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 will be stored on the secure private area of the Trust’s Office 365 The Trust will provide an overview of data breaches in the following way:

* Major data breaches and whether reported to the ICO with a full DPO report
* Minor data breaches logged where a full DPO report was not required

1. The DPO data breach reports are reviewed by the CEO and the Audit & Risk Committee (delegated from the Board of Trustees to approve the actions.)

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

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.

This will include:

**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 DPO as soon as they become aware of the error
* If the sender is unavailable or cannot recall the email for any reason, the Principal will ask the ICT department to recall it
* In any cases where the recall is unsuccessful, the Principal or 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 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 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

**31 March 2020**