Personal Data Breach Procedures

Document History	
CREATED: (Updated)	April 2018
By:	Head Teacher / SBM
Version:	1
REVIEW FREQUENCY:	Annually
APPROVED BY GOVERNING BODY:	Summer 2018
REVIEW DATE:	Currently waiting for The Enquire Learning Trust's policy to be approved. This will replace this policy. Spring 2019

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 Data Protection Officer (DPO).
- At Easterside Academy the DPO is Mrs R Parker.
- The DPO will investigate the report, 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

- The DPO will alert the Head Teacher and the Chair of Governors.
- 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).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The 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 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.
- 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 are stored in a locked filing cabinet within the Head Teacher's office.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the 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 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 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 DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The 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 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 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 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 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 in a locked filing cabinet in the Head Teacher's office.

- The DPO and Head Teacher 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

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 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 OneIT to recall it.
- In any cases where the recall is unsuccessful, the 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 and deleted.

Sensitive e-mail sent via e-mail unsecured and un-protected

- Passwords should never appear in the same e-mail as the secure document
- All sensitive data should be password protected.

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- All sensitive data should be password protected.
- School laptops should only be taken out of school if authorised and signed out by the Head Teacher / SBM on the Academy's form.
- Laptops should not be left overnight in a staff member's car.
- When travelling from school to home, laptops should be locked in the car's boot and not left in sight.
- Staff with authorised laptops to work from home should regularly bring the laptop into school to ensure it gets regular updates from the network, including security updates.
- Staff members should alert the DPO if a laptop is stolen or hacked.

A non-encrypted USB pen being stolen or lost with sensitive personal data on

- All staff should only use authorised encrypted USB pens issued by the Academy to carry sensitive personal data.
- The Senior Leadership Team (SLT) and teachers / High Level Teaching Assistant's (HLTAs) where possible should leave all sensitive personal data on the academy's network and access it remotely from home.
- All staff are regularly up-dated and refreshed with the information regarding the storage of any Academy sensitive information.
- Staff are all informed that they cannot store any academy data on their own personnel laptops or PC's.
- Staff members should alert the DPO if this breach has occurred.

An encrypted USB pen being stolen or lost with sensitive personal data on

- Only authorised encrypted pens issued by the Academy can be used.
- All Academy owned memory pens must never be used to store staff's own personal data.
- All sensitive documents should always be password protected on issued USB pen.
- Staff members should alert the DPO if this breach has occurred.