PERSONAL DATA BREACH PROCEDURES

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO). This procedure **MUST** be followed by all of The Learning Trust's staff in the event of an actual or potential data breach.

All personal data breaches must be recorded.

- On finding or causing a breach, or a potential breach, the staff member or data processor should not attempt to investigate the matter themselves and must immediately notify the Trust's Data Protection Officer (DPO).
- The Trust's DPO is:

  Euan Imrie Email - dpo@tltrust.co.uk

- 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 Trustees, the Headteacher and the chair of governors and update them with their initial findings.

- 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.

- 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 Information Commissioner's Office (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

Notification to the Information Commissioner's Office

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

- 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 the Data Breach Register ("the Register") on the network.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours (https://ico.org.uk/for-organisations/report-a-breach/). 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.

Notification to individuals

- 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.

- If individuals are not notified, the ICO still needs to be notified unless it can be demonstrated that the breach is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel us to inform affected individuals if we consider there is a high risk.

- 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 the Register. Once the Register has been updated the updated version must be emailed immediately to the DPO. You must then verbally inform the DPO that you have updated the Register and emailed it to them.

- The 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

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 the IT department 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.

Laptop, tablet, handheld device or USB drive containing non-encrypted sensitive personal data being stolen or lost

- If a laptop, tablet, handheld device or USB drive (the Device) holding non-encrypted special category data (sensitive information) is lost or stolen, the person who was last responsible for it must immediately notify the DPO of:

    - Where it was last in their possession
    - When it was last in their possession
    - A detailed description of how it came to be lost or stolen

- If the Device has been stolen the person who was last responsible for it must immediately contact the police and report a crime. All details of the report including the crime reference number must be passed to the DPO.

- If the Device has been lost the person who was last responsible for it must immediately do all is reasonably practicable to find it. Full details of the efforts made to recover the Device must be given to the DPO.

- If access to the Device can be restricted remotely the DPO will arrange for this to be done immediately.

- The DPO will assess the likelihood of whether the Device has been permanently lost and if so contact the IT department who will attempt to permanently restore the Device to its original factory settings and remove all the sensitive data.

- If a permanent restore is not possible the DPO will log the item as permanently lost in the breaches register.

THE LEARNING TRUST

NURTURING • AMBITION • EXCELLENCE