PERSONAL DATA BREACH PROCEDURE

1. 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.

   The Trust's Personal Data Breach Procedures should be read in conjunction with both the Trust's Data & Cyber Breach Prevention Policy and the Cyber Response Plan.

   The Information Commissioner's Office (ICO) broadly defines a personal data breach as a security incident that has affected the confidentiality, integrity or availability of personal data.

1.1 All personal data breaches must be recorded in the Trust's Data Breach Register. Details should be provided of: -

- the name of the person reporting the breach,
- date/time of the breach,
- date/time of detecting the breach,
- basic information about the type of breach
- information about personal data concerned.
- details of what has already been done to respond to the risks posed by the breach should also be included.

1.2 If any member of staff, governor or director of the Academy Trust, discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, they must immediately or no later than within 24 hours of first coming to notice, inform the Trust's Data Protection Officer.

1.3 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:

  Dave Helsby, Director of IT & DPO Email - dpo@tltrust.co.uk

- The DPO will investigate the report and determine whether a breach has occurred and if so, ascertain the severity of the breach and determine if any personal data is involved/compromised. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

  - Lost
  - Stolen
  - Destroyed without consent

- Altered without consent
- Disclosed or made available where it should not have been
- Made available to unauthorised people
- Accessed by someone without permission

1.4 Examples of personal data breaches include:

- Sending personal data to the wrong recipient via email.
- Lost laptops or other mobile devices which hold personal data.
- Hacking of passwords, email accounts, networks and systems.
- Loss or theft of hard copies which include personal data.

1.5 The DPO will alert the Trustees, the CEO, the Headteacher and the Chair of Governors and update them with their initial findings.

1.6 If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the Trust, then the DPO will initiate an internal investigation to consider whether the Data & Cyber Breach Prevention Policy (and other relevant policies, e.g. Staff ICT Acceptable Use Policy) was followed, and whether any alterations need to be made to internal procedures as a result.

1.7 Where the risks are higher, the priority must then be to close or contain the breach to mitigate/minimise the risks to those individuals affected by it. The DPO will make all reasonable efforts, assisted by relevant staff members, or data processors where necessary, to identify the cause of the breach to help with containment and minimise the impact of the breach.

1.8 The DPO will assess the potential consequences and risks, and how likely they are to happen by determining:

- how much data is involved,
- the personal nature and sensitivity (as defined in the Data Protection Act 2018) of the data,
- what has happened to it,
- whether it is protected or encrypted,
- whether backups are in place,
- whose data is compromised and how.

1.9 The DPO may need input from IT Support, HR, our legal advisers, and in some cases contact with external third parties and will involve the relevant Cyber Recovery/Response Team to assist with this process as and when necessary.

1.10 All Trust staff, governors and trustees are expected to work in partnership with the Data Protection Officer in relation to assessing the risks, containment and recovery, and notification of breaches.

1.11 Assistance may be required to ensure containment. The DPO (and if required, the Cyber Recovery/Response Team), will implement further action to recover lost or damaged data and contain further data loss – e.g. by taking systems offline, isolating infected devices, blocking access to compromised accounts and changing any related access codes, backing up and encrypting all existing data.

1.12 Where appropriate, the police and/or ICO may need to be notified of the security breach. The DPO and, if required, the Cyber Recovery/Response Team, will assess the situation and make this decision, including whether any affected individuals need to be notified. This must be judged on a case-by-case basis.

1.13 The ICO has a self -assessment tool to help determine whether the Trust needs to report a personal data breach to the ICO: -

ICO - Personal Data Breach Self -assessment Tool

1.14 When making the decision the DPO (and where applicable the Cyber Recovery/Response Team) 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

1.15 The Trust's Cyber Response Plan contains communication templates to assist in this situation and all of the following contact details:

- Trust & all schools
- Insurance
- Cyber security support provider
-

- External agency
- Response team contact and access information
- Personnel with server access

1.16 The DPO and the Cyber Recovery/Response Team will need to consider what steps need to be taken to mitigate the potential harm to individuals or the school community – this could include physical safety, emotional wellbeing, reputation, finances, identity or private affairs, and any threats to public reputation or general operations.

2. Notification to the Information Commissioner's Office

2.1 If it is likely that there will be a risk to people's rights and freedoms, i.e. where the data is classed as high risk to individuals, the DPO must notify the ICO immediately.

2.2 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").

2.3 The ICO has established two processes to support the reporting of personal data breaches under the UK GDPR and DPA 2018. There is a self-assessment option to determine if the breach should be reported (https://ico.org.uk/for-organisations/report-a-breach/). If the breach is reportable, there is a personal breach notification form available in English and Welsh which must be completed and sent to casework@ico.org.uk.

2.4 Where the ICO must be notified, the DPO will do this within 72 hours after becoming aware of the data breach. If over 72 hours, the DPO must provide reasons to the ICO for the delay. As required, the DPO will set out:

2.4.1 A description of the nature of the personal data breach including, where possible:

- How and when the breach occurred.
- What data it involved and whether containment measures are in place
- 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 where appropriate.

2.5 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.

3. Notification to individuals

3.1 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 by email or letter, all individuals whose personal data has been breached. The notification will explain what happened, what information was affected and what steps are being taken to prevent this from happening again:

- The communication will include 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

3.2 In certain circumstances, where appropriate, the DPO will give clear and specific advice to individuals on the steps they can take to protect themselves, and what the Trust are willing to do to help them.

3.3 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.

3.4 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

3.5 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)

3.6 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.

3.7 The DPO shall investigate whether or not the data breach was a result of human error or a systemic issue and see how a recurrence can be prevented.

3.8 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 and a report made to the CEO.

4. How to prevent Data Breaches

Active steps should be taken to reduce the possibility of personal data breaches occurring. These may include:

- having mandatory data protection training in place for all staff that includes how to recognise and report a personal data breach;
- ensuring staff have an awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails;
- having appropriate controls in place to protect personal data (e.g. ensuring devices are password protected).

5. 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.

5.1 Sensitive Information being disclosed via email (including safeguarding records)

5.1.1 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.

5.1.2 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.

5.1.3 If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it.

5.1.4 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.

5.1.5 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.

5.1.6 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.

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

5.2.1 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

5.2.2 Please note that as detailed in the Data and Cyber Breach Prevention Policy, the Trust does not allow the use of personal data on USB drives.

5.2.3 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.

5.2.4 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.

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

5.2.6 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.

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

5.3 Review of the Trust's policies and procedures following a breach

5.3.1 A review of the relevant Trust policies and procedures will be carried out following a data breach.

5.3.2 This could involve updating the Trust's Cyber Response Plan, reviewing the Data retention Policy or conducting additional training for staff.

5.3.3 The DPO will be responsible for ensuring there has been compliance with relevant regulations and legislation throughout the process and reviewing the efficiency and effectiveness of the Data and Cyber Breach Prevention Policy. This process should be reviewed at regular intervals to keep it up-to-date.

Updated March 2022
Reviewed by Author, no changes made March 2023
SW &DH reviewed and updated 12 February 2024
Approved by the Trustee Resources Panel 13 March 2024