Data Breach Policy (LLT)

LYDIATE LEARNING TRUST

ENGAGE, ENABLE, EMPOWER

Origination	*Authorised by*	*Policy Date*	*Review Date*	*Page 1 of 8*
JDA	***Board***	***Jan 26***	***Jan 29***	

Data Breach Policy (LLT)

1. Introduction

Lydiate Learning Trust (The Trust) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the Trust of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

2. Definitions

2.1 Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

2.2 Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.3 Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

2.4 Data Subject

Person to whom the personal data relates.

2.5 ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

3. Examples of a Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

4. Responsibility

- **All Staff:** must report any suspected breach immediately to their designated School PA / Business Manager representative (School Representative). If they are unavailable, email hrsupport@lydiatlearning.co.uk.
- **The People and Culture team:** responsible for overseeing this policy and developing data-related policies and guidelines. They hold overall responsibility for breach notification to the DPO of any breach and recording.
- **The Data Protection Officer (DPO):** (see below) determines whether a breach has occurred and whether it is to be reportable to the ICO.

  The Data Protection Officer (DPO): SchoolPro TLC Limited
  Address: Unit 1b Aerotech Business Park, Bamfurlong Lane, Cheltenham, United Kingdom, GL51 6TU
  Email: DPO@SchoolPro.uk
  Web: https://schoolpro.uk/
  Telephone: 01452 947633

- **Headteachers:** responsible for ensuring adherence of this policy by staff within their School and ensuring breach notification processes are in place.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

5. Security and Data-Related Policies

Staff should refer to the following policies that are related to this data breach policy: -

- **Security Policy** which sets out the Trust's guidelines and processes on keeping personal data secure against loss and misuse.
- **Data Protection Policy** which sets out the Trust's obligations under UK GDPR about how they process personal data.
- **Cyber Security Policy** which sets out the Trust's obligations and guidelines for Cyber Security issues.

These policies are also designed to protect personal data and can be found on Lydiate Learning Trust website.

6. Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO. Breach reporting is encouraged throughout the Trust and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals.

- On finding or causing a breach, or potential breach, the staff member must report it immediately to the School Business Manager / PA Representative in the first instance. Where this is not possible, report to the Headteacher.

- The School Business Manager / PA should then inform the People and Culture Team email: hrsupport@lydaitelearning.co.uk.

- The People and Culture team will log the breach immediately to the DPO Data Breach database and they will seek advice from the DPO to 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 People and Culture team and School Representative will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the DPO and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at paragraph 7.

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen based on the investigation and advise further.

- The DPO in conjunction with the People and Culture team 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.

  They will also consider the following factors to determine whether additional steps are required (such as notifying the ICO and/or affected individuals):

  - Type and sensitivity of the data involved.
  - Volume of data affected.
  - Categories and number of individuals impacted.
  - Likely consequences for affected individuals after containment.
  - Existing protections (e.g., encryption, password protection, pseudonymisation).
  - What has happened to the data.
  - What the data could reveal to a third party.
  - Potential consequences for the Trust.
  - Any wider implications or risks.

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

- The People and Culture team will ensure the decision is documented on the Breach log (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 Breach-Log in electronic format.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website. As required, the report 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 Trust will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to

have further information. The People and Culture team or DPO will submit the remaining information as soon as possible

- The Trust 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 Trust 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 Trust 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 Trust 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 are in the Breach-Log document in electronic format.

- The DPO and the People and Culture team will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

7. Actions to Minimise the Impact of Data Breaches

An example of the actions we will take to mitigate the impact of a data breach are set out below, focusing especially on a breach involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

7.1 Sensitive information being disclosed via email (including safeguarding records):

- If special category data (sensitive information) is accidently 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 report 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 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.

7.2 Other types of breach might include:

- Details of pupil premium children being published on the Trust or school website.
- Non-anonymised pupil data or staff pay information being shared with trustees.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.

8. Preventing Future Breaches

Once the data breach has been dealt with, the Trust will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether it is necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken.
- To update the data breach register.
- To debrief governors/management following the investigation.

9. Failure to Report a Breach

Breach of this policy will be treated as a disciplinary offence and may result in action under the Trust's Disciplinary Policy and Procedure, up to and including summary dismissal depending on the seriousness of the breach.

In addition, failure to report a personal data breach when required by law can result in significant financial penalties imposed by the Information Commissioner's Office (ICO). Under UK GDPR, fines may amount to the higher of €20 million or 4% of the organisation's total global annual turnover, in addition to any fines for the breach itself.

10. Training

The Trust will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

11. External Audit and Monitoring

We work closely with our appointed external audit partner to conduct independent audits of our data protection practices. These audits help ensure compliance and identify areas for improvement.

The Trust will regularly monitor the effectiveness of this policy and all related procedures. A full review and update will be carried out on a scheduled basis to maintain best practice standards.

Our monitoring process includes assessing how policies and procedures operate in practice and evaluating their effectiveness in reducing risks to the Trust. This proactive approach ensures continuous improvement and robust data protection.

12. Document Version Control Log

Approver	The Board
Date of approval	
Policy owner	Executive Director of People and Culture
Policy authors	Executive Director of People and Culture
Version	2.0
Date of next review	January 2029
Summary of changes in this review	• Aligned to the example and guidance provided by our new DPO School Pro. • Included reference to the rule that failure to report could result in a fine.
Related policies and documents	• Data protection policy • Retention Policy • Privacy notices