Data Breach Notification Policy

OUR TRUST PRAYER

Heavenly Father,
Let peace, friendship and love grow in our schools.
Send the Holy Spirit to give excellence to our learning,
love to our actions and joy to our worship.
Guide us to help others, so that we may all
Learn, Love and Achieve,
Together with Jesus.

Amen

1. Policy Statement

1.1 The Liverpool Diocesan Schools Trust (our Trust) is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.2 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.3 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2. About this policy

2.1 This policy informs all of our **workforce** on dealing with a suspected or identified data security breach.

2.2 In the event of a suspected or identified breach, our Trust must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

2.3 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

2.4 Our Trust must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

2.5 Failing to appropriately deal with and report data breaches can have serious consequences for our Trust and for **data subjects** including:

2.5.1 identity fraud, financial loss, distress or physical harm;
2.5.2 reputational damage to our Trust; and
2.5.3 fines imposed by the ICO.

3. Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in Appendix 1 to this policy.

4. Identifying a Data Breach

4.1 A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

4.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

4.2.1 Leaving a mobile device on a train;
4.2.2 Theft of a bag containing paper documents;
4.2.3 Destruction of the only copy of a document;
4.2.4 Sending an email or attachment to the wrong recipient;
4.2.5 Using an unauthorised email address to access personal data;
4.2.6 Leaving paper documents containing personal data in a place accessible to other people.

5. Internal Communication

Reporting a data breach upon discovery

5.1 If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Headteacher, Designated Data Protection Lead and Data Protection Officer (DPO) immediately.

Alison Tennant, Trust Data Protection Officer
E: dataprotection@ldst.org.uk

5.2 The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

5.3 If it is considered to be necessary to report a data breach to the ICO then our Trust must do so within 72 hours of discovery of the breach.

5.4 Our Trust may also be contractually required to notify other organisations of the breach within a period following discovery.

5.5 It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the Headteacher, Designated Data Protection Lead and DPO immediately.

5.6 Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

5.7 In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach Minimisation

5.8 The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be **minimised**. The focus will be on containing any data breach, and recovering any **personal data**. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

5.8.1 shutting down IT systems;
5.8.2 contacting individuals to whom the information has been disclosed and asking them to delete the information; and
5.8.3 recovering lost data.

Breach Investigation

5.9 When our Trust has taken appropriate steps to minimise the extent of the data breach it must **commence an investigation** as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

5.10 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

5.10.1 what data/systems were accessed;
5.10.2 how the access occurred;
5.10.3 how to fix vulnerabilities in the compromised processes or systems;
5.10.4 how to address failings in controls or processes.

5.11 Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why and reviewing policies and procedures.

Breach Analysis

5.12 In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform our Trust as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to **analyse the nature of the data breach**.

5.13 Such an analysis must include:

5.13.1 the type and volume of **personal data** which was involved in the data breach;
5.13.2 whether any **special category personal data** was involved;
5.13.3 the likelihood of the **personal data** being accessed by unauthorised third parties;
5.13.4 the security in place in relation to the **personal data**, including whether it was encrypted;
5.13.5 the risks of damage or distress to the **data subject**.

5.14 The breach notification form annexed to this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of our Trust in deciding whether or not to report the breach.

6. External communication

6.1 All external communication is to be managed and overseen by the Headteacher, Designated Data Protection Lead and DPO.

Law Enforcement

6.2 The Headteacher, Designated Data Protection Lead and DPO will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

6.3 The DPO and Headteacher will coordinate communications with any law enforcement agency.

Other organisations

6.4 If the data breach involves **personal data** which we process on behalf of other organisations then we may be contractually required to notify them of the data breach.

6.5 Our Trust will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

6.6 If our Trust is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then our Trust has 72 hours to notify the ICO if the data breach is determined to be notifiable.

6.7 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The Headteacher, Designated Data Protection Lead and DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

6.7.1 the type and volume of **personal data** which was involved in the data breach;
6.7.2 whether any **special category personal data** was involved;
6.7.3 the likelihood of the **personal data** being accessed by unauthorised third parties;
6.7.4 the security in place in relation to the **personal data**, including whether it was encrypted;
6.7.5 the risks of damage or distress to the **data subject**.

6.8 If a notification to the ICO is required then see part 7 of this policy below.

Other supervisory authorities

6.9 If the data breach occurred in another country or involves data relating to data subjects from different countries then the Headteacher, Designation Data Protection Lead ad DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

6.10 When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by our Trust.

6.11 The communication will be coordinated by the Headteacher, Designated Data Protection Lead and Trust DPO and will include at least the following information:

6.11.1 a description in clear and plain language of the nature of the data breach;
6.11.2 the name and contact details of the Headteacher, Designated Data Protection Lead and Trust DPO;
6.11.3 the likely consequences of the data breach;
6.11.4 the measures taken or proposed to be taken by our Trust to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

6.12 There is no legal requirement to notify any individual if any of the following conditions are met:

6.12.1 appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);

6.12.2 measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

6.12.3 it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

6.13 For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Press

6.14 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the Headteacher, Designated Data Protection Lead or DPO.

6.15 All press enquiries shall be directed to our Trust's Central Services Team (0151 705 2175).

7. Producing an ICO Breach Notification Report

7.1 All members of our **workforce** are responsible for sharing all information relating to a data breach with the Headteacher, Designated Data Protection Lead and Trust DPO, which will enable the annexed Breach Notification Report Form to be completed.

7.2 When completing the attached Breach Notification Report Form all mandatory (* / red) fields must be completed, and as much detail as possible should be provided.

7.3 Our Trust DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

7.4 If any member of our **workforce** is unable to provide information when requested by our Trust DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

7.5 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

7.6 The ICO requires that our Trust send the completed Breach Notification Form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or

by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

8. Evaluation and response

8.1 Reporting is not the final step in relation to a data breach. Our Trust will seek to learn from any data breach.

8.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

Review Schedule

Policy Author	Data Protection Officer
Policy Approver	Audit and Risk Committee
Current Policy Version	1.4
Policy Effective From	March 2024
Policy Review Date	By March 2026

Revision Schedule

Version	Revisions	By whom
1.0	Original document produced	DPO
1.1	Minor updates to contact information	DPO
1.2	None	DPO
1.3	Minor changes to annex 1 (clarifying baseline information required for initial reporting to the DPO).	DPO
1.4	Minor change to DPO contact information. New breach notification form (appendix 2) and Data Breach Flowchart (appendix 3).	DPO

APPENDIX 1 - Definitions

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by our Trust such as staff and those who volunteer in any capacity including Governors, Trustees, Members and parent helpers

APPENDIX 2 – LDST Internal Breach Notification

About the breach

1. **Please describe what happened and how the incident occurred.** Give details about the events leading up to breach, it could be someone being called away from their desk and leaving confidential documents that was visible to a parent attending a meeting at school.

2. **How did you discover the breach?** This could be a parent contacting school or someone finding a lost bag on a train.

3. **Was the breach caused by a cyber incident?** A cyber attack is a breach with a clear online or technological element that involves a third party with malicious intent. For example: incidents involving phishing or malware attacks.

☐ Yes

☐ No

☐ Don't know

4. **When did the breach happen?** This is the date of the breach and won't necessarily be the same date/time as school discovering the breach.

Date: Time:

5. **When did you discover the breach?** This is when someone in school found out about the breach.

Date: Time:

6. **Categories of personal data included in the breach (tick all that apply)**

☐ Data revealing racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Sexual orientation data

☐ Gender reassignment data

☐ Health data

☐ Basic personal identifiers, eg name, contact details

☐ Identification data, eg usernames, passwords

☐ Economic and financial data, eg credit card numbers, bank details

☐ Official documents, eg driving licences, passports

☐ Genetic or biometric data

☐ Criminal convictions, offences

☐ Other (please give details below)

Please give additional details if you can to help us understand the nature of the personal data included in the breach:

7. **Number of personal data records concerned.** This could be all CPOMS records for all current year groups or it could involve more than one record type. For example, it could be all records relating to current Year 6/9 pupils/students or a full archive file of students who have left secondary education 6 years ago.

8. **How many data subjects could be affected?** This could be the number of affected pupils/students only but you need to consider if parent/carer data is also included.

9. **Categories of data subjects affected (tick all that apply)**

☐ Students/Pupils

☐ Parents/Carers

☐ Staff

☐ Governors/Volunteers

☐ Contractors/Suppliers

☐ Other (please give details below)

10. **Had the staff member involved in this breach received data protection training in the last two years?** There is GDPR training available via National College and resources available on SharePoint.

☐ Yes

☐ No

☐ Don't know

11. **If there has been a delay in reporting this breach to the Trust DPO, please explain why.** A member of staff may have been aware of the breach but was worried about reporting it. It is important that staff know that this is about us all helping to contain the breach and mitigate risk of harm but it is also about our concern for them as it can be a very stressful and anxious time for the individual involved. We understand that mistakes happened and unless the person has purposefully and maliciously cause the breach, they will not be held responsible.

12. **Have you taken action to contain the breach or limit its impact? Please describe these remedial actions.** This could be asking for e-mails sent in error to be permanently deleted, documentation returned to school, removing something from the website/social media…

13. **Have you told data subjects about the breach?**

☐ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects due to the urgency

☐ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway

☐ No – but we are planning to because we have determined it is likely there is a high risk to data subjects but would also like advice from the DPO

☐ No – we determined the incident did not meet the threshold for communicating it to data subjects but would also like advice from the DPO

Person making this report

Name:

Email:

Phone:

Sending this form

Please send to dataprotection@ldst.org.uk with 'Personal data breach notification' in the subject field.

APPENDIX 3 – Data Breach Management Flowchart

LDST Breach Management Flowchart

Personal data breach occurs

Breach reported in school to Head, DPO, SBM or other. Complete Internal Data Breach Notification Form

Identify: Initial risk analysis (Headteacher/ DPO)

Is the breach likely to result in a risk to people's rights and freedoms?

Yes – then the breach should be reported by the Trust DPO within 72 hours of school being aware

No – the breach is not reportable

Agree breach action plan – depending on the scale and nature of the breach

Consider contacting the Data Subject(s) ***Mandatory if there is a high risk to the rights and freedoms of individuals***

Notify relevant Trustees and Governors

Contain: Take URGENT action to recover the data, mitigate the loss, reduce the risks

Do any other external agencies need to be informed? Police, social care?

Begin any internal procedures

Fulfil any communication and updating obligations or agreements with relevant parties, e.g. Data Subject (s) & ICO

Report outcomes → **Identify operational needs** → **Implement strategies** → **Review impact of changes**

Have you completed National College GDPR training?
Have you read and understood our Data Protection Policies?
If not, speak with your Headteacher immediately for further information.