GREENSHAW
LEARNING TRUST

Greenshaw Learning Trust
Data Breach Procedure

Greenshaw Learning Trust
Data Breach Procedure

Contents

PART A 3

1.1. Application 3

1.2. Approval and review 3

1.3. Terminology 3

1.4. Responsibilities 4

1.5. Associated policies and procedures 4

PART B 5

2. What is a Data Breach? 5

3. Dealing with a Data Breach 5

4. Assessing the Breach 6

5. Recording the Breach

6. Preventing Future Breaches 7

Annex A – Judicium / ICO Data Breach Reporting Form 8

PART A

1.1. Application

This GLT Data Breach Procedure applies to the Greenshaw Learning Trust as a whole and to all the schools in the Trust and the Trust Shared Service, in accordance with and pursuant to the Communications Policy of the Greenshaw Learning Trust.

The Greenshaw Learning Trust, including all the schools, their Trustees, governors and staff, must abide by this GLT Data Protection Policy.

This Procedure is subject to the Trust's Scheme of Delegation for Governance Functions. If there is any ambiguity or conflict then the Scheme of Delegation and any specific alteration or restriction to the Scheme approved by the Board of Trustees takes precedence.

In implementing this Procedure and associated policies and procedures the governing body, Headteacher and school staff, and Trust Shared Service staff, must take account of any advice or instruction given to them by the GLT Data Protection Officer, the GLT CEO or Board of Trustees.

If there is any question or doubt about the interpretation or implementation of this Policy, the GLT CEO should be consulted.

1.2. Approval and review

Maintenance of this Procedure is the responsibility of the GLT CEO.

This Procedure was approved by the Board of Trustees on: 9th February 2024.

This Procedure is due for review by: February 2027.

1.3. Terminology

The Trust means the Greenshaw Learning Trust (GLT).

- School means a school within the Greenshaw Learning Trust.
- Headteacher means the headteacher or principal of the school.
- CEO means the chief executive officer of the Greenshaw Learning Trust.
- Governors and Trustees includes governors, Trustees, non-governor members of Trust Committees and members of the Trust Panel.
- Governing body means the committee of the Board of Trustees to which Trustees have delegated appropriate powers and functions relating to the governance of the school.
- GLT Data Protection Officer means SchoolPro TLC.
- School Data Protection Lead means the point of contact for data protection matters for members of staff, students and parents within the school
- Data Subject means an individual about whom such personal information is stored.
- Data Controller means the organisation storing and controlling information regarding data subjects which is Greenshaw Learning Trust.

In this policy references to the Greenshaw Learning Trust will be read as including the Trust Shared Service and all schools in the Greenshaw Learning Trust.

References in this Procedure to a school in the Trust should also be read as the Trust Shared Service for services, functions and members of staff of the Trust that are not contained within a school budget and/or are not the responsibility of a Headteacher and/or Governing Body. With respect to the Trust Shared Service, references in this Procedure to the responsibilities of the Headteacher and Governing Body should be read as the GLT CEO and the GLT Board of Trustees respectively.

1.4. Responsibilities

It is the responsibility of the governing body and Headteacher of each school, and the Board of Trustees and GLT CEO for the Trust Shared Service, to ensure that their school/service and its staff adhere to this GLT Data Breach Procedure; in implementing this Procedure the governing body, Headteacher and Trust staff must take account of any advice given to them by the GLT Data Protection Officer, GLT CEO and/or Board of Trustees.

For the purposes of data protection legislation the Greenshaw Learning Trust is the Data Controller, and can be contacted by writing to Greenshaw Learning Trust, ORU Sutton, Throwley Way, Sutton, SM1 4AF.

The GLT Data Protection Officer is: SchoolPro TLC.

Email: DPO@schoolpro.uk
Address: Unit 1b Aerotech Business Park, Bamfurlong Lane, Cheltenham, United Kingdom, GL51 6TU
Telephone: 01452 947633
Lead Contact: Ben Craig

Each Headteacher will appoint a School Data Protection Lead to be the point of contact for data protection matters for members of staff, students and parents of their school, and to liaise with the GLT Data Protection Officer. The name and contact details must be provided to the GLT Data Protection Officer and will be made available on the school website or by contacting the school.

1.5. Associated policies and procedures

- This GLT Data Breach procedure is a constituent part of the GLT Data Protection Policy.

.

PART B

2. What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Examples of data breaches are:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data;
- leaving a PC unattended so a student or staff member can access data;
- inadvertently displaying data to a classroom on a screen;
- sending information about a child to the wrong address or email address;
- any breach of the data protection principles.

3. Dealing with a Data Breach

All members of staff in Greenshaw Learning Trust must be aware of what constitutes a data breach and what action to take in the event of a breach.

All breaches must be reported to the school / service Data Protecton Lead, in the first instance and as soon as discovered and reported to the GLT Data Protection Officer through the SchoolPro platform by following the instructions on the 'Breaches' link on the platform.

For most breaches the “General Breach” form can be completed.

If a breach needs to be reported to the Information Commissioner’s Office (ICO) then please complete the “ICO Report Form”, as found in Annex A. If unsure, do complete the “General Breach” form and the GLT Data Protection Officer will be able to advise further.

Once notified, the GLT Data Protection Officer shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Further details may be required by the GLT Data Protection Officer from the school / service to make an assessment. Unless the GLT Data Protection Officer concludes that there is unlikely to be any a risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the school Data Protection Lead unless a delay can be justified. The GLT Data Protection Officer may require the ICO Report Form to be completed on SchoolPro and will provide this to the person making the report or the Data Protection Lead within the school / service.

Where the Data Protection Lead is fully satisfied that a breach is non-reportable, low risk and doesn't require further action, they can log the breach on the SchoolPro platform without seeking advice from the GLT Data Protection Officer. This should only be done in limited circumstances and if ever unsure, the Data Protection Lead should seek advice of the GLT Data Protection Officer.

Where a breach is determined as reportable, the GLT Data Protection Officer shall inform the Information Commissioner of:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries which shall be the GLT Data Protection Officer;
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Lead within the school / service under the guidance and advice of the GLT Data Protection Officer shall notify data subjects of the breach without undue delay., unless the data would be unintelligible to those not authorised to access it or measures have been taken to mitigate any risk to the affected individuals.

The affected data subjects shall be informed of:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

4. Assessing the Breach

Once initial reporting procedures have been carried out, the school /service will carry out all necessary investigations into the breach.

The school Data Protection Lead will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. They will identify ways to recover, correct or delete data (for example notifying insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the school in consultation with the DPOservice will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;

- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school / service; and
- Any other wider consequences which may be applicable.

5. Reporting Breaches

Regardless of severity, all breaches should be logged with the DPO. The majority of these will be through the DPO portal which each School Data Protection Lead has access to.

If reportable to the ICO, the form should be completed and sent to the DPO for them to forward to the ICO. This must be completed within 72 hours of the school becoming aware of the breach.

6. Preventing Future Breaches

Once the data breach has been dealt with, the school Data Protection Lead will consider its security processes with the aim of preventing further breaches. In order to do this, they 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 awareness within members of staff 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.
- Update the data breach register.
- Submit a report to the Headteacher who will report to the Governing Body.

All breaches will be reported to the Board of Trustees by the GLT Data Protection Officer and any recommendations for further training or a change in procedure shall be reviewed by the Board of Trustees and a decision made about implementation of those recommendations.

Reporting and monitoring

Reports on data breaches and summary data, with any recommendations with suggestions for further training or changes to policy will be reported regularly to the Board of Trustees or appropriate Committee.