Greenshaw Learning Trust
Data Breach Procedure

May 2018

This Greenshaw Learning Trust Procedure applies to the Greenshaw Learning Trust as a whole and to all the schools and service units in the Trust, in accordance with and pursuant to the Data Protection Policy of the Greenshaw Learning Trust. The Greenshaw Learning Trust, including all the schools and services within the Trust, their Trustees, governors and staff, must abide by this Procedure.

This Procedure must be read in conjunction with the GLT Data Protection Policy; all the terms of the GLT Data Protection Policy apply to the interpretation and implementation of this Procedure; if there is any ambiguity or conflict the GLT Data Protection Policy must be followed.

This Policy is subject to the Scheme of Delegation approved for the school or service. If there is any ambiguity or conflict then the Scheme of Delegation and any specific Scheme or alteration or restriction to the Scheme approved by the Board of Trustees takes precedence.

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

Approval and review:

This Procedure is the responsibility of the GLT CEO.
This Procedure was approved by the Board of Trustees on: 23 May 2018.
The Procedure was updated by the GLT CEO to reflect changes to Trust titles and terminology and the appointment of 'Judicium' as DPO from 1 January 2021.
This Procedure is due for review by: May 2021.

Greenshaw Learning Trust
Data Breach Procedure

1.1 Responsibilities, approval and review

It is the responsibility of the Governing Body and Headteacher of each school, and the Board of Trustees and GLT CEO for Trust Shared Service, to ensure that their school/service and its staff adhere to this 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, Grennell Road, Sutton, SM1 3DY.

The GLT Data Protection Officer is: Judicium Consulting Limited.
Email: dataservices@judicium.com
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

Each school and the Trust Shared Service will appoint a lead to be the point of contact for data protection matters for staff, students and parents, and to liaise with the GLT Data Protection Officer. The name and contact details must be provided to the Data Protection Officer.

This Procedure was approved by the Board of Trustees on: 23 May 2018. The Policy was updated by the GLT CEO to reflect changes to Trust titles and terminology and the appointment of 'Judicium' as DPO from 1 January 2021.

This Procedure is due for review by: May 2021.

1.2 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.
- Governing Body (GB) means the committee of the Board of Trustees to which Trustees have delegated appropriate powers and functions relating to the governance of the school.

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

1.3 Application

This Procedure applies to the Greenshaw Learning Trust as a whole and to all the schools and service units in the Trust, in accordance with and pursuant to the Data Protection Policy of the Greenshaw Learning Trust. The Greenshaw Learning Trust, including all the schools and services within the Trust, their Trustees, governors and staff, must abide by this GLT Data Protection Procedure.

In implementing this Procedure and associated school policies and procedures the Governing Body, Headteacher and school staff must take account of any advice or instruction given to them by the GLT Data Protection Officer, the GLT Directors of Education, the GLT CEO or Board of Trustees.

If there is any question about the interpretation or implementation of this Procedure, the GLT Data Protection Officer, GLT CEO or appropriate GLT Director of Education should be consulted.

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.

4. DEALING WITH A DATA BREACH

All 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 GLT Data Protection Officer as soon as discovered. The form attached as Annex A must be completed and emailed to dataservices@judicium.com.

If a data breach occurs in a school, the school data protection lead must be alerted and he/she should complete the form attached as Annex A and return it to the Data Protection Officer.

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.

Unless the GLT Data Protection Officer concludes that there is unlikely to be any 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 GLT Data Protection Officer unless a delay can be justified. The GLT Data Protection Officer may require a further form to be completed and will provide this to the person making the report.

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 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 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 GLT Data Protection Officer shall inform data subjects of:

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

The GLT Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented.

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.

Annex A

Data Breach Report

Name	
Name of school	
Contact details	

Please complete the following fields with as much information as possible:

Nature of the breach:
Date of the breach:
What sort of data has been breached? **How many people may be affected?**

What measures can be taken immediately or have been taken to mitigate the risk to the individuals?
What security measures were in place that will protect the information?

Please submit this form by email to the Data Protection Officer at dataservices@judicium.com