GREENSHAW
LEARNING TRUST

Greenshaw Learning Trust Information Security Policy

ALWAYS
LEARNING

Contents

PART A

1.1. Application

This GLT Information Security Policy 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 Information Security Policy.

This Policy 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 policy 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 Policy is the responsibility of the GLT CEO.

This Policy was approved by the Board of Trustees on: 16 December. 2022
This Policy is due for review by: 28 February 2025.

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 Judicium Consulting Ltd.

In this policy 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.

References in this Policy to a school in the Trust should also be read as the Trust Shared Service for services, functions and 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 Policy to the responsibilities of the Headteacher and Governing Body should be read as the GLT CEO and the Trust Shared Services Committee 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 Information Security Policy; in implementing this Policy 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.

The Board of Trustees has the ultimate responsibility for Information Security in the Trust.

The School's Governing Body has been given delegated responsibility for the oversight of Information Security within their school.

The GLT Chief Executive Officer (CEO) has overall responsibility for ensuring compliance with information security in the day to day running of the trust:
William Smith. Email: wsmith@greenshawlearningtrust.co.uk

The Headteacher of each school has been given delegated responsibility for information security in their school.

Each Headteacher will appoint:
• A School Data Protection Lead to be their point of contact for data protection and information security.

The GLT Head of IT has special responsibility for the maintenance and implementation of the Trust's IT and Cyber Security Policy and Procedures: Richard Hatch. Email: rhatch@greenshawlearningtrust.co.uk

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
Address: 72 Cannon Street, London, EC4N 6AE Telephone: 020 3326 9174
Lead Contact: Craig Stilwell

1.5. Associated policies and procedures

The following Trust policies and procedures are directly related to and complement this GLT Information Security Policy:

- GLT Data Protection Policy including the:
    - GLT Data Retention Procedure.
    - GLT Subject Access Request Procedure.
    - GLT Data Breach Procedure.
    - GLT Privacy Notices.
    - GLT CCTV Use Procedure.
- GLT Staff and Volunteer Code of Conduct.
- GLT Trustee and Governor Code of Conduct.
- GLT Hybrid Working Policy.

The following Trust policies and procedures are constituent parts of the Information Security Policy

- GLT Cyber Security Procedure

Part B

1. Context and Principles

Greenshaw Learning Trust (GLT) is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by GLT to achieve this, including to:

- To protect against potential breaches of confidentiality;
- To ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- To support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- To increase awareness and understanding of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

2. Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

3. General Principles

All data stored by GLT is classified appropriately (including, but not limited to personal data, sensitive personal data and confidential information). Further details on the categories of data can be found in the GLT Data Protection Policy and GLT Privacy Notices. All data so classified must be handled appropriately in accordance with its classification.

All data stored within our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption (full details regarding protection of electronic data can be found in our GLT Cyber Security Procedures).

All staff have an obligation to report actual and potential data protection compliance failures to the Data Protection Officer (full details can be found in our Data Protection Policy and Data Breach Procedure).

4. Physical Security and Procedures

The Headteacher will ensure that:

- Paper records and documents containing personal information, sensitive personal information and confidential information are securely locked away to avoid unauthorised access when not in use.
- Paper documents containing confidential personal information are not left where there is general access unless there is legal reason to do so and/or relevant consents have been obtained.
- Particular care is taken if documents have to be taken out of school or Trust buildings and staff refer to the expectations laid out in the GLT Hybrid Working Policy when working from home.

The Headteacher will ensure that measures are taken to ensure the physical security of GLT building/s and storage systems, including:

- Regular checks of the buildings and storage systems to ensure they are maintained to a high standard.
- CCTV cameras and alarm systems are in use.
- Visitors to GLT schools and buildings are required to follow the school's signing in procedures.

and should not be left alone in areas where they could have access to confidential information.

5. Computers and IT

The Headteacher will ensure that:

- They maintain the security and integrity of all IT Systems and the data stored thereon (including but not limited to the security, integrity and confidentiality of that data), taking advice from the GLT Head of IT in accordance with the Cyber Security Procedure.
- All IT Systems are installed, maintained, serviced, repaired and upgraded only with the approval of the GLT Head of IT.
- All members of staff comply with all relevant parts of the GLT Cyber Security Procedures at all times when using GLT IT Systems.

6. Communications, Transfers, Internet and Email Use

The Headteacher will ensure that:

- Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and GLT cannot accept liability for the material accessed or its consequence.
- All personal information and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by or recorded delivery.
- Postal and email addresses and numbers are checked and verified before information is sent to them. In particular, take extra care with email addresses where auto-complete features may have inserted incorrect addresses.
- All members of staff comply with all relevant parts of the GLT Cyber Security Procedures at all times when sending or receiving emails.
- That all members of staff maintain confidentiality when speaking in public places.
- Confidential information is marked 'confidential' and circulated only to those who need to know the information in the course of their work for GLT.
- Personal or confidential information is not removed from GLT buildings except where the removal is temporary and necessary. When such removal is necessary all reasonable steps must be taken to ensure that the integrity of the information and the confidentiality are maintained, including that it is:
  a) not transported in see-through or other un-secured bags or cases;
  b) not read in public places (e.g., waiting rooms, cafes, trains, etc.); and
  c) not left unattended or in any place where it is at risk (e.g., in car boots, cafes, etc.).
- All members of staff comply with all relevant parts of the GLT Hybrid Working Policy at all times when accessing personal or confidential data from home.

7. Reporting Security Breaches

A security breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In circumstances of a data breach or suspected data breach, the GLT Data Breach Procedures must be followed