

Greenshaw Learning Trust

Information, Data and Cyber Security Policy and Procedures

Information, Data and Cyber Security Policy and Procedures

Greenshaw Learning Trust Information, Data and Cyber Security Policy and Procedures	1
Information, Data and Cyber Security Policy and Procedures	2
Part One: Information, Data and Cyber Security Policy	3
1.1 Application and Scope	3
1.2 Approval and Review	3
1.3. Terminology	3
1.4 Data Controller and Data Protection Officer	4
1.5 Responsibilities	4
1.6 Policy Intent	5
1.7 Data Protection Principles (UK GDPR)	5
1.8 Conditions for processing in the First Data Protection Principle	6
1.9 Personal Data	6
1.10 Use of Personal Data by Greenshaw Learning Trust	7
1.11 Confidentiality of Pupil Concerns	8
1.12 Transfer of Data Outside the UK	8
1.13 Transfer of Data Outside the European Economic Area (EEA)	9
1.14 Importance of Adherence in the Current Threat Landscape	9
1.15 Complaints	9
PART TWO: Operational Procedures	10
2. Data Classification and Processing	10
2.1 Data Classification and Confidentiality	10
2.2 Biometric Data Usage (Special Category Data)	10
2.3 Data Subject Rights	10
2.4 Subject Access Requests (SARs) and Our Response	11
3. Operational Security and Cyber Controls	12
3.1 Physical Security Procedures	12
3.2 IT Systems and Cyber Attack Prevention Controls	13
3.3 Staff Controls and Conduct	13
3.4 Communications and Email	13
3.5 Monitoring and Access to Work Accounts and Drives	14
3.6 Training	
	14

4. Data Retention and Deletion	15
4.1 Retention Periods	15
4.2 Deletion Procedures	15
5. Incident Management	16
5.1 Reporting Security Breaches or Cyber Incidents	16
5.2 Cyber-Attack Incident Management Plan	16
5.3 Reporting to Regulators (ICO)	16

Part One: Information, Data and Cyber Security Policy

1.1 Application and Scope

This Policy applies to the Greenshaw Learning Trust (GLT) as a whole, including all schools in the Trust and the Trust Shared Service.

All schools, the Trust Shared Service, their Trustees, Governors, and staff must abide by this Policy and its associated Procedures. This Policy is subject to the Trust's Scheme of Delegation. In case of ambiguity or conflict, the Scheme of Delegation (and any specific alteration approved by the Board of Trustees) takes precedence.

It is the responsibility of the Headteacher of each school, and the GLT CEO for the Trust Shared Service, to ensure that their school/service and its staff adhere to this GLT Information, Data and Cyber 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 and the GLT CEO.

This Policy and its Associated Procedures are written using guidance, legislation, and best practices from UK General Data Protection Regulation and the Data Protection Act 2018, Safeguarding Legislation, Guidance from the Information Commissioner Office (ICO) and requirements from the Joint Council for Qualifications (JQC) Regulations for Approved Centres.

1.2 Approval and Review

- Maintenance of the Policy and its Associated Procedures is the responsibility of the GLT CEO
- This Policy and its Associated Procedures were approved by the GLT Board of Trustees on: XXXX

- This Policy and its Associated Procedures are due for review: XXXX (3 years from approval date)

1.3. Terminology

- The Trust means the Greenshaw Learning Trust (GLT).
- School means a school within the Greenshaw Learning Trust.
- CEO means the Chief Executive Officer of the Greenshaw Learning Trust.
- Headteacher means the headteacher or principal of the school.
- 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 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

1.4 Data Controller and Data Protection Officer

Data Controller:

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

Data Protection Officer

The GLT Data Protection Officer is: SchoolPro TLC

Email: DPO@schoolpro.uk

Address: Unit 1b, Aerotech Business Park, Bamfurlong Ln, Staverton Bridge, Cheltenham GL51 6TU

Telephone: 01452 947633

Lead Contact: Ben Craig

The Trust is registered with the Information Commissioner's Office (ICO) under registration number

ZA246923. All schools within the Trust are registered under this same registration.

1.5 Responsibilities

- **The Board of Trustees:** Has the ultimate responsibility for Information Security in the Trust.
- **The GLT CEO:** Has overall responsibility for ensuring compliance with information security in the day-to-day running of the Trust and is responsible for the maintenance of this Policy and its associated Procedures.
- **The Headteacher** (of each school): Has delegated responsibility for information, data and cyber security in their school. Each Headteacher will appoint a School Data Protection Lead 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.
- **School Data Protection Lead:** is the main point of contact for data protection matters for staff, pupils and parents of their school and liaises with the Data Protection Officer
- **All Staff, Governors, and Trustees:** All must contribute towards cyber security and are responsible for adherence to this Policy. A member of staff, Trustee, or Governor may be subject to disciplinary action if they breach this procedure.

1.6 Policy Intent

The Greenshaw Learning Trust is dedicated to ensuring the security of all information that it holds and implements the highest standards to achieve this. The core purposes of this policy are to:

- Protect against potential breaches of confidentiality.
- Ensure that all information assets and IT facilities are protected against damage, loss, or misuse.
- Support compliance with UK law (including UK GDPR and Data Protection Act 2018) and Trust procedures applying to the processing of data.
- Increase awareness and understanding of information security and the responsibility of all staff to protect the confidentiality and integrity of the information that they handle.

Information Security is defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. This Policy addresses risks from cyber criminals and associated cyber security risks, ensuring appropriate action is taken should the Trust fall victim to cyber-crime

1.7 Data Protection Principles (UK GDPR)

The Trust will adhere at all times to the seven data protection principles as laid down in the UK General Data Protection Regulation (UK GDPR):

1. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed fairly, lawfully, and in a transparent manner, requiring a lawful basis (processing condition).
2. **Purpose Limitation:** Personal data shall be collected for specific, explicit, and legitimate purposes only and shall not be further processed in a manner incompatible with those purposes.
3. **Data Minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.
4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date.
5. **Storage Limitation:** Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes.
6. **Integrity and Confidentiality (Security):** Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
7. **Accountability:** The Trust is responsible for and must be able to demonstrate compliance with the other six principles.

In addition to this, the Greenshaw Learning Trust is committed to ensuring that at all times, anyone

dealing with personal data shall be mindful of an individual's rights under the law. This means that the Greenshaw Learning Trust will:

- inform individuals as to the purpose of collecting any information from them, as and when it is asked for, in accordance with the GLT privacy notices;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Data Retention Procedure;
- ensure that when information is authorised for disposal it is disposed of appropriately;
- ensure appropriate security measures are taken to safeguard personal information, whether it is held in paper files or on electronically, and follow the relevant security requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- follow the GLT Subject Access Request Procedure for responding to requests for access to personal information known as 'subject access requests'; and
- report any breaches of the UK GDPR in accordance with the GLT Data Breach Procedure.

1.8 Conditions for processing in the First Data Protection Principle

The conditions which enable the Greenshaw Learning Trust to process data lawfully under the first

data protection principle are:

- The individual has given consent that is specific to the particular type of processing activity, and that consent was informed, unambiguous and freely given.
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
- The processing is necessary for the performance of a legal obligation to which the Trust is subject.
- The processing is necessary to protect the vital interests of the individual or another individual or body.
- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of an official authority vested in the Trust.
- The processing is necessary for a legitimate interest of the Greenshaw Learning Trust or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned

1.9 Personal Data

‘Personal data’ is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. For example, if asked for the number of female employees, and there is only one female

employee, this would be personal data if it was possible to obtain a list of employees’ names from the school website. A sub-set of personal data is known as ‘special category personal data’.

This special category personal data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual’s sex life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person;
- data relating to criminal offences and convictions.

Special category personal information is given special protection, and additional safeguards apply if this information is to be collected and used. Biometric data is considered special category data and can only be processed using explicit consent (see section 2.3). The Greenshaw Learning Trust and its schools will not make use of facial recognition data. Information relating to criminal convictions shall only be held and processed where the Trust has legal authority to do so. The Greenshaw Learning Trust does not intend to seek or hold sensitive personal data about staff or pupils except where it has been notified of the information, or it is obtained via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice.

No person is under any obligation to disclose their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member, or details of their sexual life, criminal offences or convictions (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements or applications for employment).

Photography and video captured (for example from CCTV or the recording of meetings) or audio recordings (for example from recorded phone calls) are treated as personal data and processed in accordance with this policy. Headteachers will hold an addendum detailing school specific elements. Separate consent may be required for specific uses such as marketing or press publications.

1.10 Use of Personal Data by Greenshaw Learning Trust

The Greenshaw Learning Trust holds personal data on pupils, staff and other individuals such as visitors.

In each case, the personal data will be treated in accordance with the data protection principles as outlined above. School Data Protection Leads will provide the appropriate GLT privacy notice to all data subjects:

- Privacy Notice for parents and carers.
- Privacy Notice for pupils
- Privacy Notice for younger pupils (under 13)
- Privacy Notice for staff.
- Privacy Notice for governors and trustees
- Privacy Notice for visitors

If any data subject wishes to limit or object to any use of their personal data they should notify the GLT Data Protection Officer in by email or in writing. The GLT Data Protection Officer will acknowledge the notification in writing. If, in the view of the GLT Data Protection Officer, the objection cannot be maintained, the individual will be given written reasons why the Greenshaw Learning Trust cannot comply with their request.

Staff

The data held on staff is used to comply with legal obligations placed on the Greenshaw Learning Trust in relation to employment of staff and the education of children in a school environment. The Greenshaw Learning Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material where consent to this has been provided. Personal data will also be used when giving references. Data will be retained in line with the guidance from the Information and Records Management Society's Information Toolkit for Schools.

Trustees and Governors

The personal data held about governors and trustees is collected and used to comply with legal obligations placed on the Greenshaw Learning Trust by the Companies Act 2006, the Charities Act 2011, and in accordance with the Articles of Association and Funding Agreements of the Trust and the Academy Trust Handbook.

Other Individuals

The Greenshaw Learning Trust may hold personal information in relation to other individuals who have contact with the Trust or any of its schools, such as volunteers and visitors.

1.11 Confidentiality of Pupil Concerns

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Greenshaw Learning Trust will maintain confidentiality unless the GLT Data Protection Officer has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the GLT Data Protection Officer believes disclosure will be in the best interests of the pupil or other pupils. If any member of staff receives a request to withhold disclosure of personal data to parents or guardians this should be reported to the School Data Protection Lead. The School Data Protection Lead will report to and take advice from the GLT Data Protection Officer.

1.12 Transfer of Data Outside the UK

The Greenshaw Learning Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct. Any transfer of data outside the UK must be authorised by the GLT Data Protection Officer.

1.13 Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. The Greenshaw Learning Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country. If any member of staff believes that data might be transferred outside the EEA they must notify the School Data Protection Lead who will take advice from the GLT Data Protection Officer.

1.14 Importance of Adherence in the Current Threat Landscape

In today's rapidly evolving digital world, the importance of strictly adhering to the Greenshaw Learning Trust's Information, Data and Cyber Security Policy and Procedures cannot be overstated. The threat landscape is constantly shifting, with cyber criminals employing increasingly sophisticated tactics to exploit vulnerabilities. Schools and educational trusts, holding sensitive personal data for students and staff, are prime targets for cyber-attacks, data breaches, and other security incidents.

Failure to comply with this policy can lead to severe consequences, including:

- **Breaches of Confidentiality:** Unauthorised access to, or disclosure of, personal and sensitive data, potentially harming individuals and eroding trust.
- **Reputational Damage:** Significant damage to the Trust's and its schools' reputation, impacting public perception and stakeholder confidence.
- **Financial Penalties:** Substantial fines and legal costs imposed by regulatory bodies like the Information Commissioner's Office (ICO) for non-compliance with data protection legislation.

- **Operational Disruption:** Cyber-attacks such as ransomware can halt critical school operations, impacting teaching, learning, and administrative functions.
- **Legal and Ethical Obligations:** A failure to protect data breaches the Trust's legal obligations under UK GDPR and the Data Protection Act 2018, as well as its ethical duty to safeguard the information entrusted to it.

Every member of staff, Trustee, and Governor plays a critical role in maintaining a robust security posture. By understanding and diligently following the guidelines outlined in this policy, we collectively contribute to protecting our information assets, safeguarding personal data, and ensuring the continued integrity and security of the Greenshaw Learning Trust. Vigilance, awareness, and strict adherence are our strongest defenses against current and emerging cyber threats.

1.15 Complaints

In the first instance, complaints should be made through either the School or Trust Complaints Procedures, as appropriate.

PART TWO: Operational Procedures

2. Data Classification and Processing

2.1 Data Classification and Confidentiality

All data stored is classified appropriately (e.g., personal data, sensitive personal data, and confidential information).

- Personal Data: Information that identifies an individual.
- Special Category Personal Data: This sensitive sub-set of data includes information relating to physical or mental health, race/ethnic origin, religious beliefs, and biometric data for the purpose of uniquely identifying a natural person. [cite_start]Additional safeguards apply to its collection and use.
- Access Control: All data must be available only to members of staff with a legitimate need for access. Confidential information must be marked 'confidential' and circulated only to those who need to know it.

2.2 Biometric Data Usage (Special Category Data)

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person, such as fingerprints.

- Processing Basis: To lawfully process biometric data, the Trust must have a legal basis for processing personal data and a separate explicit consent (which satisfies the fair processing conditions).
- Purpose: GLT collects and uses biometric data for purposes including enabling the efficient operation of school canteen provision and a school library.
- Facial Recognition: The Greenshaw Learning Trust does not currently make use of facial recognition data.
- Objection/Alternatives: If a member of staff, student, or parent objects to the processing of their biometric data, the school will provide reasonable alternatives which allow access to the same facilities.
- Withdrawal of Consent: Consent can be withdrawn at a later stage, in writing or by email, to the School Data Protection Lead.

2.3 Data Subject Rights

The Trust is committed to complying with all individual rights under the law. These include the right to:

- Subject Access Request (SAR): Individuals have the right to confirmation as to whether personal data is processed and, if so, access to that data and supplementary information. Requests should be submitted by email to DPO@SchoolPro.uk

- **Object to Processing:** Individuals can object to processing based on public interest or legitimate interest grounds. The GLT DPO will assess the objection within two school days of receipt.
- **Rectification:** Individuals have the right to request the rectification of inaccurate data or the completion of incomplete data without undue delay.
- **Erasure (Right to be forgotten):** An individual has the right, in certain circumstances (e.g., data is no longer necessary, consent is withdrawn), to have personal data permanently erased without undue delay.
- **Portability:** Individuals may request their personal data in a structured, commonly used, and machine-readable format if the processing is based on consent or performance of a contract.

The GLT DPO can be contacted with regards to any of the above on DPO@SchoolPro.uk. Privacy notices for Staff, Visitors, Parents & Carers, Students (age 13+) and Younger Students can be found on the GLT website, or on any school website by visiting the GDPR and Privacy pages.

2.4 Subject Access Requests (SARs) and Our Response

The Greenshaw Learning Trust is committed to upholding the rights of individuals regarding their personal data, including the right to access the information held about them. This right is exercised through a Subject Access Request (SAR).

Scope of a SAR:

A SAR grants an individual the right to obtain confirmation as to whether their personal data is being processed, and if so, to access that data and supplementary information. The scope of a SAR can be broad and may include:

- **Personal Information:** Any information that identifies the individual, such as names, addresses, contact details, dates of birth, and unique identifiers.
- **Sensitive Personal Data (Special Category Data):** This includes information relating to physical or mental health, race/ethnic origin, religious beliefs, biometric data, and sexual orientation.
- **Educational Records:** Information related to a student's academic progress, attendance, disciplinary actions, and support needs.
- **Employment Records:** For staff, this could include contracts, performance reviews, disciplinary records, and payroll information.
- **Communications:** Emails, letters, Google chat messages, or other forms of communication where the individual is the subject or a significant participant.
- **CCTV Footage:** If the individual is identifiable in CCTV recordings.

- **Audio Recordings:** where a phone call has taken place the individual and this has been recorded. This would be included as a transcript of the call.
- **Opinions and Assessments:** Records of opinions or assessments made about the individual. Maintain a professional, factual, and evidence-based tone at all times.
- **Information** held in both electronic and manual filing systems, including data held on any system controlled by the organisation (Bromcom, CPOMS, NeoPeople etc)

Receiving a SAR:

- **Identification:** Any request from an individual for their personal data, or data relating to another individual they are authorised to act on behalf of, should be treated as a SAR. Requests do not need to be in writing or use specific terminology.
- **Submission:** While individuals have the right to submit a SAR in any format, we encourage submission by email to DPO@SchoolPro.uk to ensure efficient processing.
- **Initial Action:** Upon receipt of a SAR, the School Data Protection Lead (or the GLT DPO if received directly) must immediately log the request and acknowledge its receipt.

Responding to a SAR:

- **Verification of Identity:** Before disclosing any personal data, the Trust must take reasonable steps to verify the identity of the requester. This may involve asking for proof of identity or clarification of information already held.
- **Scope of Request:** The GLT DPO will work with the relevant school or service to identify and gather all personal data pertaining to the data subject that falls within the scope of the request. This includes data held in electronic and manual filing systems.
- **Exemptions:** Certain exemptions may apply under data protection legislation, which could permit the Trust to withhold some information. Any application of exemptions will be carefully considered and documented by the GLT DPO.
- **Third-Party Information:** Where a SAR includes information relating to other individuals, appropriate steps will be taken to redact or anonymise that information, or to seek consent from the third party, to protect their privacy rights.
- **Timeline:** The Trust will respond to a SAR without undue delay and, in any event, within one calendar month of receiving the request. This period may be extended by a further two months for complex or numerous requests, with the individual being informed of the extension and the reasons for it within the initial one-month period.
- **Format of Response:** The information will be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

- **No Fee:** Generally, no fee will be charged for fulfilling a SAR. However, a reasonable fee may be charged for manifestly unfounded or excessive requests, or for further copies of information already provided.

Record Keeping:

- All SARs, the steps taken to fulfill them, and the final response provided will be meticulously documented and retained in accordance with the Trust's data retention policies.

3. Operational Security and Cyber Controls

3.1 Physical Security Procedures

The Headteacher must ensure that measures are taken to ensure the physical security of GLT building(s).

- **Secure Storage:** Paper records containing personal information must be securely locked away to avoid unauthorised access when not in use.
- **Visitor Procedures:** Visitors must follow signing-in procedures and should not be left alone in areas where they could have access to confidential information.
- **Off-site Working:** Staff must refer to the GLT Hybrid Working Policy when working from home. When removing personal/confidential information temporarily, it must not be transported in unsecured bags, read in public places, or left unattended/at risk.

3.2 IT Systems and Cyber Attack Prevention Controls

The Headteacher must ensure that the School IT Lead has in place systems and controls to mitigate the risk of a cyber-attack, following the advice of the GLT Head of IT. Cyber-attacks can take the shape of hacking, phishing emails, malware, viruses, or ransomware attacks.

Controls include (but are not limited to):

- **Access and Password Management:** Use of strong passwords and Multi-Factor Authentication (MFA). MFA will be enabled for all accounts that access awarding bodies' online systems. Devices used for MFA must not be shared by multiple staff members.
- **Network Security:** Correctly configured Firewalls, Anti-virus and malware software , Anti-Spam filtering for email, and Internet Filtering.
- **Data Protection:** Encryption (where there is a risk of devices or data falling into the wrong hands). Processes for deleting or disabling unused redundant user accounts.
- **Backups:** Secure backups of all data, both onsite and hosted, with a minimum of 3 copies, including one that is offsite or offline.

- **Maintenance:** Automatic updates for systems and applications. IT Systems are installed, maintained, and upgraded only with the approval of the GLT Head of IT.

3.3 Staff Controls and Conduct

Every member of staff, Trustee, and Governor must:

- **Passwords:** Choose a password with a minimum of 8 characters, including upper and lower case, numbers, and punctuation. Keep passwords secret and never reuse one. Never save passwords to local web browsers on shared devices. Never share login/password details or additional factor/authentication codes with anyone else.
- **Security Bypass:** Not turn off or attempt to circumvent any security measures (antivirus, firewalls, web filtering, encryption).
- **Permissions:** Only grant necessary permissions to third party applications and only use trusted services. Regularly review and remove access for applications that are no longer used. Never approve or authenticate a login request that you did not initiate.
- **Misuse:** Not install software without authorisation. Avoid clicking on links to unknown websites. Misuse includes any malicious/illegal action, accessing inappropriate content, excessive personal use, or removing data/equipment without permission.
- **Reporting:** Report any security or data breach, suspicious activity, or mistake made that may cause a cyber security breach, to the School IT Lead, as soon as practicable from the time of the discovery or occurrence.

3.4 Communications and Email

- **Encryption:** All personal and sensitive personal information should be encrypted before being sent by email or sent by recorded delivery.
- **Verification:** Postal and email addresses must be checked and verified before sending information. Take extra care with auto-complete features.
- **Appropriate Use of Email / Chat:** Staff should use email professionally and responsibly, understanding that all communications on Trust systems are considered Trust property. When composing emails, particularly those concerning staff members, students, or sensitive matters, staff should adopt a "Write Everything as If It Will Be Published" mentality. This means assuming that any email, chat, or document created could eventually be read by the individual concerned (e.g., as part of a Subject Access Request). Therefore, maintain a professional, factual, and evidence-based tone at all times. Avoid speculative, informal, or inappropriate language that could be misinterpreted or cause harm if disclosed.

3.5 Monitoring and Access to Work Accounts and Drives

The Greenshaw Learning Trust reserves the right to monitor and access work email accounts and drives, including all content stored within them, where it is deemed appropriate and necessary to do so. This may occur in circumstances such as:

- **Investigation of Policy Breaches:** To investigate suspected breaches of this Information, Data and Cyber Security Policy, other Trust policies, or legal obligations.
- **Legal and Regulatory Compliance:** To ensure compliance with legal or regulatory requirements, including responding to legitimate requests from law enforcement or regulatory bodies, or in response to a Subject Access Request (SAR) or Freedom of Information (FOI) Request.
- **System Security and Integrity:** To protect the integrity and security of the Trust's IT systems, data, and network from threats such as malware, phishing, or unauthorised access.
- **Business Continuity:** In cases where a staff member is absent, or where there is a legitimate business need to access information critical to the Trust's operations.
- **Safeguarding:** To fulfill the Trust's safeguarding responsibilities and protect the welfare of students and staff.

Any monitoring or access will be conducted in a manner that is proportionate, lawful, and respects the privacy of individuals as far as is reasonably practicable, in accordance with relevant legislation and guidance. Staff should be aware that all communications and data stored on Trust systems are considered Trust property and should be used for legitimate work-related purposes only.

3.6 Training

All staff, trustees and Governors are required to complete annual, up to date, cyber security and data protection training, and refresher training if appropriate which may include; when there is a change to the law, regulation or policy; where significant new threats are identified; and in the event of an incident affecting the school or any third parties with whom data is shared.

3.7 Suppliers who process data on behalf of the Trust

The GLT DPO holds a Data Impact Assessment for all suppliers who process data on behalf of the trust. These are reviewed regularly by the Compliance Team. The **GLT Procurement Policy** outlines our data security principles and must be adhered to when tendering for a new supplier. To ensure the robust protection of data when engaging with third-party suppliers who process data on behalf of the Trust, the following procedures and considerations are in place:

- **Due Diligence and Risk Assessment:** Before engaging any new supplier, a thorough due diligence process will be conducted under the GLT Procurement Policy. A Data Impact Assessment (DIA) will be completed for all suppliers, evaluating the risks associated with their processing activities.
- **Data Processing Agreements (DPAs):** All suppliers who process personal data on behalf of the Trust must enter into a formal Data Processing Agreement (DPA). This agreement will clearly define the scope of processing, the responsibilities of both the Trust (as data controller) and the supplier (as data processor), and the technical and organisational measures the supplier must implement to ensure data security. The DPA will also include provisions for data breaches, data subject rights, and data retention/deletion.
- **Ongoing Monitoring and Review:** The Compliance Team, with the support of the GLT DPO, will regularly review the performance and compliance of all suppliers. This includes:
 - Periodic audits of supplier security practices.
 - Reviewing the DIAs and DPAs to ensure they remain current and effective.
 - Monitoring for any changes in a supplier's security posture or data processing activities.
 - Ensuring that any sub-processors used by the supplier are also subject to appropriate data protection safeguards.
- **Incident Management with Suppliers:** In the event of a data breach or security incident involving a supplier, the DPA will outline clear procedures for immediate notification to the Trust, investigation, and cooperation in mitigating the impact and fulfilling reporting obligations to regulatory bodies.

Adherence to these procedures is critical to maintaining the security and confidentiality of the data entrusted to the Greenshaw Learning Trust, even when processed by third parties.

4. Data Retention and Deletion

4.1 Retention Periods

Personal data is only retained for as long as necessary for the purpose concerned. GLT follows the **Information and Records Management Society's Information Toolkit for Schools**.

- **Biometric Data Retention:** If consent has been withdrawn, or once a student or staff member leaves, the biometric data will be deleted from the system within 72 hours.
- **Other Data:** The maximum retention period for an Educational Record is 25 years from the date of birth if it is the final school. Most employment records are kept for 6 years from the end of employment.

4.2 Deletion Procedures

- Confidential Documents: Anything that contains personal information should be treated as confidential. Paper confidential documents must be shredded, or placed in confidential waste bins or sacks for collection.
- Electronic Deletion: The GLT Data Protection Officer must be consulted to ensure electronic deletion is carried out effectively.

5. Incident Management

5.1 Reporting Security Breaches or Cyber Incidents

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. Any member of staff, Trustee, or Governor has an obligation to report actual and potential data protection compliance failures. All breaches must be reported to the School/Service Data Protection Lead in the first instance, as soon as discovered, and then reported to the GLT DPO. Any member of staff, Trustee, or Governor aware of or suspecting a cyber-attack or cyber incident must immediately notify the GLT Head of IT or the appropriate School IT Lead.

5.2 Cyber-Attack Incident Management Plan

The Headteacher must ensure their school has and implements an incident management plan encompassing four stages:

1. Containment and Recovery: Immediately reporting the attack to the GLT Head of IT and investigating to mitigate damage and recover lost data.
2. Assessment: Confirming what data has been affected, how sensitive it is, and identifying the consequences.
3. GLT Head of IT Decision: Deciding if the cyber-attack needs to be reported to regulators (e.g., ICO/DfE) and/or parents/colleagues.
4. Evaluation and Response: Considering improvements to data security and evaluating future threats.

The contingency plan should cover all aspects of exam administration and delivery and should incorporate annual testing of the secure recovery and business continuity processes for assessment administration systems. Any actual or suspected compromise of an awarding body's online systems must be reported immediately to the relevant awarding body

5.3 Reporting to Regulators (ICO)

- DPO Assessment: Once notified, the GLT DPO shall assess the breach's extent, risks to data subjects, and security measures in place.

- 72-Hour Deadline: Unless the DPO concludes there is unlikely to be a risk to individuals, the breach must be notified to the Information Commissioner's Office (ICO) within 72 hours of the breach coming to the attention of the School Data Protection Lead.
- High Risk Notification: If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, the DPO shall notify data subjects of the breach without undue delay