Data Protection Policy

Date ratified	May 2025
Committee Responsible for Policy	Business Committee
Date to be updated	May 2026
Headteacher Signature	
Chair of Governors/ Committee Signature	

Holy Trinity has adopted the Merton model Data Protection Policy November 2024 v14.

Introduction

Our school is committed to protecting and responsibly managing all data we hold. This policy outlines how we collect, use, and safeguard information in compliance with UK GDPR and the Data Protection Act 2018.
We maintain transparent data practices across all school operations, including:

- Student and pupil records
- Employee and staff information
- Data sharing with external organisations (Local Authorities, Department for Education, other schools, social services, and law enforcement agencies when required)

This policy provides staff and governors with clear guidelines for data protection compliance. It works alongside our HR policy, which specifically addresses personal data management for job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees.

To ensure robust data protection, we:

- Implement practical, documented procedures
- Maintain clear organisational policies
- Subscribe to Merton's Data Protection Officer (DPO) Service Level Agreement

Our DPO advises on data protection obligations and can be contacted at schoolsDPO@merton.gov.uk

Legislative Framework

This policy has due regard to all relevant legislation and statutory requirements, including, but not limited to:

Core Data Protection and Privacy

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations (PECR)
- Protection of Freedoms Act 2012 (particularly regarding biometric data in schools)
- The Environmental Information Regulations 2004

Education Specific

- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The School Standards and Framework Act 1998
- Education Act 2011
- Education and Skills Act 2008
- Keeping Children Safe in Education (statutory guidance)
- The Children Act 1989 & 2004
- Special Educational Needs and Disability (SEND) Code of Practice: 0 to 25 years

Digital and Security

- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- The Network and Information Systems Regulations 2018
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Employment and Rights

- Human Rights Act 1998
- The Equality Act 2010
- Employment Rights Act 1996
- Public Records Act 1958
- Limitation Act 1980 (particularly regarding records retention)

Financial and Administrative

- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Companies Act 2006 (for academies/trusts)
- Charities Act 2011 (for academies/trusts)
- The Public Contracts Regulations 2015 (for procurement record-keeping)
- The Procurement Act 2023

In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.

Breaches of data protection legislation can result in significant monetary penalties and damage to reputation, as well as the risk of real harm to people whose data is handled in an unfair or unlawful way.

Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.

Guidance and Standards

This policy has been developed with regard to the following guidance and standards:

Core Data Protection

- ICO 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO 'Data Sharing Code of Practice'
- National Cyber Security Centre (NCSC) 'Data Security Guidance for Schools'

Education Sector Specific

- Department For Education 'Data Protection: A toolkit for schools'
- Department For Education 'Meeting digital and technology standards in schools and colleges'
- Department for Education 'Keeping Children Safe in Education'

Information Security

- ISO/IEC 27001 Information Security Management principles
- NCSC's '10 Steps to Cyber Security'
- ICO 'Security Outcomes'

Specific Processing Activities

- ICO 'Age Appropriate Design Code' (for digital services used by children)
- ICO guidance on handling Subject Access Requests in education settings

- Department for Education 'Protection of children's biometric information in schools'

This policy will be implemented in conjunction with the following policies:

- Online Safety Policy
- Safe Use of Cameras and Images Policy
- Freedom of Information Policy and Model Publication Scheme
- Child Protection and Safeguarding Policy
- Data Retention Policy
- AI policy (due 2025)

Scope and Responsibilities

This Policy applies to all staff, including temporary staff, consultants, governors, volunteers, and contractors, and anyone else working on behalf of our school.

All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to our Data Protection Officer.

All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it.

Our Data Protection Officer is responsible for advising us about our data protection obligations, dealing with breaches of this policy, including suspected breaches, identified risks, and monitoring compliance with this policy.

Applicable Data

Article 4 states that "'personal data' means any information relating to an identified or identifiable natural person ('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.

The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data.

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', This is defined as

- Genetic data.
- Biometric data.
- Data concerning health.

- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.

Principles

In accordance with the requirements outlined in the UK GDPR:

- Personal data is only processed in keeping with legal data protection principles. The principles include: data being processed lawfully, fairly and in a transparent manner; data being processed only for specific, explicit and valid purposes; data being adequate, relevant and accurate; data not being kept longer than is necessary; and data being kept secure;
- We adopt a "Privacy by Design" and "Privacy by Default" approach;
- We can demonstrate our accountability and compliance;
- The people whose data we hold (Data Subjects) understand the ways and reasons why we process their data, and can easily and fairly exercise their rights around their data;
- We only share personal data when it is fair and lawful to do so, and when we share data we do it in a safe and secure way;
- Data is not transferred outside of the UK except where the country has an 'adequacy decision' or the transfer is covered by 'appropriate safeguards', as defined in UK GDPR Article 46, or there is a specific situation that allows the transfer as defined by UK GDPR Article 49;
- All data breaches, including near misses, are managed properly and reported appropriately, so we can minimise any risks and improve practices in the future. This includes any breaches of the Data Protection Act (DPA 2018) where the individual responsible may be liable.

Accountability

This school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

We will also provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules

- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism and safeguards in place.

We will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving its security features.

Data protection impact assessments will also be used, where appropriate to document the risks, decision-making process and decisions made, including recommendations and actions.

Artificial Intelligence (AI)

Our school recognises the increasing role of artificial intelligence (AI) in education and administration. When using AI systems that process personal data, we adhere to the same data protection principles outlined in this policy. This includes ensuring transparency about AI use, maintaining data accuracy, and respecting data subject rights. We conduct Data Protection Impact Assessments (DPIAs) for new AI implementations that may pose high risks to individuals' rights and freedoms.

For more detailed information on our approach to AI, please refer to our separate AI Policy.

Data Protection Officer (DPO)

This school participates in the Merton Council DPO SLA which provides a shared DPO for Merton Schools. In addition, a member of staff will be designated Chief Privacy Officer (CPO) and this person will support the DPO.

The DPO will assist the Data Controller to inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws, monitor our compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly in relation to maintained schools.

The DPO will report to the highest level of management.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will work alongside safeguarding leads to ensure that pupil/student data is protected as required.

Lawful Processing

Legal Bases for Processing Data
The legal basis for processing data will be identified and documented prior to data being processed.

Under the UK GDPR, data will be lawfully processed under one of the following conditions (Article 6):

a) Consent of the data subject

   Example: Obtaining explicit permission to use a student's photograph on the school website.

b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

   Example: Processing staff payroll information to fulfil employment contracts.

c) Processing is necessary for compliance with a legal obligation

   Example: Sharing student information with the Department for Education as required by law.

d) Processing is necessary to protect the vital interests of a data subject or another person

   Example: Disclosing a student's medical information to emergency services in case of a life-threatening situation.

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

   Example: Collecting and maintaining student academic records as part of the school's educational responsibilities.

f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

   Example: Using parent contact details to inform them about school events or fundraising activities.

At least one of these bases must apply for the processing to be lawful. The appropriate basis may vary depending on the specific processing activity, and the school will always choose the most appropriate basis for each processing operation.

For special category data, additional conditions from Article 9 of the UK GDPR must also be met. Special Categories of Personal Data (Article 9).

Processing of special category data is prohibited unless one of the following conditions applies:

a) Explicit consent

Example: Obtaining explicit permission to process a student's health data for a school trip.

b) Employment, social security and social protection law

Example: Processing staff health information for occupational health purposes.

c) Vital interests

Example: Sharing a student's medical information with emergency services when they are unable to give consent.

d) Legitimate activities of a not-for-profit body

Example: A school alumni association processing information about members' religious beliefs.

e) Data made public by the data subject

Example: Using information a student has openly shared on a public school forum.

f) Legal claims or judicial acts

Example: Processing special category data for establishing, exercising, or defending legal claims against the school.

g) Substantial public interest

Example: Processing data about students' ethnic origins for equality monitoring purposes.

h) Health or social care

Example: School nurses processing student health data to provide care.

i) Public health

Example: Sharing student health data with public health authorities during an epidemic.

j) Archiving, research and statistics

Example: Using anonymised special category data for educational research purposes.

When processing special category data, we must have both a lawful basis under Article 6 and meet one of these conditions under Article 9. Additionally, we must document which condition we are relying on and ensure you have appropriate policy documents and safeguards in place.

For certain conditions (b, g, h, i, j), there must also be a basis in UK law, which is typically found in the Data Protection Act 2018.

Consent

When we use consent as a legal basis for processing data, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

We will ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by a data subject at any time.

The Right to be Informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, we will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within our privacy notice:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation with reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

i) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

j) the right to lodge a complaint with a supervisory authority;

k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

l) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Right of Access

Key Principles:

- **Child Requests:** For SARs concerning a child's information, we assess the child's capacity to understand their rights. If deemed capable, we respond directly to the child.
- **Identity Verification:** We verify the identity of all requestors before releasing any information to ensure data security.
- **Format and Costs:**
  - Information is provided free of charge for the first request.
  - A reasonable fee, based on administrative costs, may be charged for additional copies or for requests that are manifestly unfounded, excessive, or repetitive.
  - Electronic requests receive responses in a commonly used electronic format, transmitted securely to protect personal information.
- **Timeframes:**
  - We respond to all requests without delay, within one month of receipt.
  - For complex or numerous requests, we may extend this period by up to two additional months, informing the individual within the first month and explaining the delay.
- **Right to Refuse:** We reserve the right to refuse manifestly unfounded or excessive requests, informing the individual of this decision, the reasons, and their right to complain to the supervisory authority and seek judicial remedy within one month.
- **Large Volumes of Data:** Where we process a large quantity of information about an individual, we may ask them to specify which information their request relates to.

Additional Considerations:

- **Assistance:** We provide support to individuals who need help making a SAR, ensuring accessibility for all data subjects.
- **Record Keeping:** We maintain records of all SARs and our responses for accountability and compliance purposes.
- **Exemptions:** Some data may be exempt from SARs (e.g., information related to ongoing legal proceedings). We will inform requestors if any exemptions apply to their request.

We are committed to upholding individuals' rights to access their personal data while maintaining the security and integrity of all information we process.

The Right to Rectification

Individuals have the right to request the rectification of any inaccurate or incomplete personal data we hold about them. We are committed to ensuring that personal data is accurate and up-to-date.
Key Principles:

- **Rectification Requests:** Individuals can request corrections to their personal data if they believe it is inaccurate or incomplete.

- **Informing Third Parties:** If the corrected data has been shared with third parties, we will notify them of the rectification where possible. Additionally, we will inform the individual about these third parties if appropriate.
- **Response Timeframes:**
    - We aim to respond to rectification requests within one month of receipt.
    - If a request is complex, this period may be extended by up to two additional months. In such cases, we will inform the individual within the first month and provide an explanation for the delay.
- **Right to Refuse:**
    - If we decide not to take action on a rectification request, we will inform the individual of the reasons for this decision.
    - We will also advise them of their right to complain to the supervisory authority and seek a judicial remedy

By ensuring personal data accuracy, we uphold individuals' rights and maintain the integrity and reliability of our data processing activities.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or • statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The Right to Restrict Processing

Individuals have the right to block or suppress our processing of personal data. In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

We will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data.
- Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction Instead.
- Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We will inform individuals when a restriction on processing has been lifted.

The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller

- Where the processing is based on the individual's consent or for the performance of a Contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. We will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

We use School 2 School (S2S), provided by the Department for Education, to securely transfer pupil records to and from other schools in a machine readable format.

S2S is a secure data transfer website available to schools and Local Authorities in England and Wales.

S2S has been developed to enable all data files required by DfE or by Local Authorities on behalf of DfE or which schools need to send to each other to be sent securely.

This school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

We will respond to any requests for portability within one month.

The Right to Object

We will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests

- An individual's grounds for objecting must relate to his or her particular situation.
- We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- We will stop processing personal data for direct marketing purposes as soon as an objection is received.
- We cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, we will offer a method for individuals to object online.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Data Protection by Design and Privacy Impact Assessments

We will act in accordance with the UK GDPR by adopting a data protection by design approach and implementing technical and organisational measures which demonstrate how we has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to this school's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

- We will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

Data Breaches

The UK GDPR identifies personal data breaches as follows:

- **"Confidentiality breach"** - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **"Availability breach"** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- **"Integrity breach"** - where there is an unauthorised or accidental alteration of personal data.

The Senior Leadership Team will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of us becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at we, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in action by the Information Commissioner.

The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

Cyber Security and Cyber Incidents

We recognise the critical importance of cyber security in protecting data and maintaining operational continuity. We implement a comprehensive approach to cyber security that includes:

- Technical measures: Firewalls, anti-virus software, anti-spam software, system updates, URL filtering, secure data backups, encryption, and strong password policies.
- Staff training: Regular cyber security awareness training for all staff, covering topics such as phishing, safe browsing, and data protection.
- Access control: Implementing the principle of least privilege and using multi-factor authentication for accounts with access to sensitive data.
- Incident response plan: A regularly tested plan detailing steps to follow in the event of a cyber attack, including communication protocols, containment, and recovery processes.
- Backup strategy: Maintaining at least three backup copies of important data on at least two separate devices, with one copy stored off-site.
- Reporting: Serious cyber attacks will be reported to the appropriate authorities as required.

We conduct regular risk assessments to identify potential vulnerabilities and update our cyber security measures accordingly. All staff are required to follow our cyber security policies and report any suspicious activities or potential breaches immediately.

By prioritising cyber security, we aim to protect our school community from the operational, financial, and reputational impacts of cyber incidents and attacks

Data Security

Handling of Confidential Paper Records

Secure Storage

- Confidential paper records are stored in locked filing cabinets, drawers, or safes with restricted access. Only authorised personnel may access these secure storage areas.

Clear Desk Policy

- Staff must adhere to a strict clear desk policy, ensuring confidential documents are never left unattended or visible in areas with general access. All sensitive documents require immediate securing when not in active use, particularly outside of working hours.

Off-Site Data Protection

- The School Business Manager, Designated Safeguarding Leads, and SENCO are equipped with lockable security pouches specifically designed for transporting sensitive documents when absolutely necessary. Comprehensive training is provided on the proper use of these pouches and associated data handling risks.

Document Tracking

- A comprehensive log tracks all confidential documents removed from secure storage, recording document details, responsible personnel, and expected return dates.

Secure Disposal

- Confidential paper records are securely destroyed using cross-cut shredders or through certified secure disposal services, ensuring complete and irretrievable destruction.

Digital Alternatives

- We actively encourage transitioning to secure digital document management to minimise reliance on paper records wherever possible.

Staff Training

- Regular, comprehensive training ensures all staff understand and consistently apply confidential document handling procedures.

Visitor Management

- Visitors are never permitted unaccompanied in areas where confidential records are stored or processed.

Incident Reporting

- Immediate reporting of any potential breaches or mishandling of confidential paper records is mandatory for all staff members.

Digital Data Protection

Encryption and Access Control:

- All digital data is encrypted and password-protected, both on local hard drives and network drives. We use Advanced Encryption Standard (AES) 256-Bit Security to FIPS-197 standard for removable storage and portable devices. The LGFL GridStore System is utilised for offline backups.

Device Security:

- Encrypted removable storage and portable devices are stored in locked filing cabinets, drawers, or safes when not in use. All electronic devices are password-protected and, where possible, configured for remote blocking or deletion in case of theft or loss.

Removable Storage:

- The use of memory sticks is discouraged. When necessary, only password-protected and fully encrypted memory sticks are permitted for personal information.

Personal Devices and Accounts:

- Staff and governors are prohibited from using personal laptops, computers, devices, email accounts, or cloud storage for school business.

Network Access:

- Staff members are provided with unique, secure logins and passwords for network access. Regular password changes are enforced by the system.

Remote Access:

- Remote access to school systems is granted based on a credible business case and is facilitated through the LGFL CISCO Anywhere client. Two-factor authentication, including both 'soft' and 'hard' One-Time Passwords, is mandatory for remote network access.

Staff Training:

- Regular training is provided to all staff on digital data protection practices and the importance of maintaining data security.

Wi-Fi Access and Security

School Network Access:

- Wi-Fi access to the school network is restricted to school-owned devices only.
- All school devices use WPA3 encryption for Wi-Fi connections.

Guest Wi-Fi:

- A separate Guest Wi-Fi network is provided for staff-owned devices and visitors.
- The Guest Wi-Fi has limited access to school resources and is isolated from the main network.

Authentication:

- All Wi-Fi networks require secure authentication methods (e.g., username/password, certificate-based).

Network Monitoring:

- We actively monitor Wi-Fi usage for unusual activities or potential security threats.

Regular Updates:

- Wi-Fi infrastructure is regularly updated to address security vulnerabilities.

Usage Policy:

- All users must adhere to our Acceptable Use Policy when connected to any school Wi-Fi network.

Network Access and File Management

Principle of Least Privilege:

- Access to files and folders on the school network is granted on a 'need-to-know' basis, adhering to the principle of least privilege.

Role-Based Access Control (RBAC):

- We implement a robust RBAC system, where permissions are assigned based on staff roles, responsibilities, and seniority.

Granular Permissions:

- File and folder permissions are set at a granular level, ensuring precise control over who can view, edit, or delete specific information.

Regular Access Reviews:

- We conduct periodic reviews of access rights to ensure they remain appropriate and up-to-date.

Monitoring and Auditing:

- File access and user activities on the network are continuously monitored and logged.
- Regular audits are performed to detect any unusual access patterns or potential security breaches.

Data Classification:

- Files are classified according to their sensitivity, with stricter access controls for more sensitive information.

Access Request Process:

- A formal process is in place for requesting and approving changes to access rights.

Secure Authentication:

- Multi-factor authentication is required for accessing sensitive areas of the network.

Training and Awareness:

- Staff receive regular training on the importance of data security and their responsibilities in maintaining it.

Email Security:

- We use encrypted email services for sending sensitive information externally.
- Staff are trained to use caution when sharing confidential data via email.
- Circular emails to parents use blind carbon copy (bcc) to protect recipient privacy.

Secure File Transfer:

- For transferring sensitive documents, we utilise the LGfL USO File Exchange (USO-FX) service.
- This allows secure file transfers between schools and Local Authorities.

Parent Communication:

- Our school primarily uses our Management Information System (MIS) for parental contact, ensuring secure and direct communication.

Document Encryption:

- When sending sensitive documents electronically, we use password protection and encryption.

Fax Usage:

- Fax usage has been phased out due to security concerns and outdated technology.

Staff Training:

- All staff receive regular training on secure communication practices and data protection.

Alternative Secure Methods:

- We employ other secure communication methods as appropriate, such as secure messaging systems or encrypted file-sharing platforms.

Taking Information Offsite

- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from school premises accepts full responsibility for the security of the data.

Where data is taken off site for educational visits all staff will ensure:

- all risk assessments and other data sensitive documentation are managed securely on the day of the visit.

- When not being referred to, all documentation such as risk assessments should be kept securely in staff members bags during the visit to prevent a potential data breach.
- Different documentation should be kept separately in plastic wallets to minimalize a breach in data should any document be mislaid e.g. risk assessments, tickets, maps, groupings.
- Any pupil sensitive information given to parents/visitors supporting the school visit should be on a 'need to know' basis only e.g. only the medical conditions of the children in their group should be shared.
- All documentation given to additional adults should be collected back at the end of the visit by the party leader.

Sharing Data
Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

This school takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Visitors

- Visitors to areas containing sensitive information are always supervised.
- The physical security of our buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Safeguarding

The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible.

Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.

Publication of Information

This school publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

This school will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to we website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV and Photography

We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

We notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

We will always indicate our intentions for taking photographs of pupils and will retrieve permission before publishing them.

If we wish to use images/video footage of pupils in a publication, such as our website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

Data Retention

Data will not be kept for longer than is necessary. We document all information we hold and dispose of data according to our retention schedule.

The Department for Education recognise that further guidance is required in this area and we will incorporate any new standard approach into our record management practice as it emerges. [1]

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of we may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be cross cut shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

A certificate of destruction will be obtained when computer hard drives that have held personal information are disposed of.

DBS Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Definitions

Definitions used by this school (drawn from the UK GDPR):

Material scope (Article 2) – the UK GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – Controllers and processors established in the UK who process personal data, regardless of whether the processing takes place in the UK or not.

Controllers and processors not established in the UK that process personal data of data subjects who are in the UK, where the processing activities are related to:

- Offering goods or services to data subjects in the UK, or
- Monitoring the behaviour of data subjects as far as their behaviour takes place within the UK.

Processing of personal data in a place where UK law applies by virtue of public international law.

[1] "work will be done to develop a consistent voice that supports schools by generating and sharing exemplar data retention policy." DFE "Data Protection a toolkit for Schools" April 2018

Article 4 definitions:

Establishment – The main establishment of a controller or processor is typically where its central administration is located. However:

1. For controllers: If decisions about data processing purposes and means are made in a different establishment that can implement them, that location becomes the main establishment.
2. For processors: If there's no central administration, the main establishment is where the primary processing activities take place.

Controllers based outside the UK may need to appoint a UK representative, depending on their processing activities.

Personal data – any information relating to an identified or identifiable natural person ('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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK law, the controller or the specific criteria for its nomination may be provided for by UK law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the UK GDPR defines a child as anyone under the age of 18 years old. For online services (information society services) offered directly to children, the UK has set the age of consent at 13 years old.

The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Data Protection Officer (DPO) – person responsible for informing and advising an organisation about their data protection obligations, and monitoring their compliance with them.

Chief Privacy Officer or **champion** (CPO) – person responsible for implementing and developing data protection as communicated by the DPO.