Wimbledon Chase Primary School

Empowering individuals to thrive and contribute positively in a diverse and ever-changing world

Data Protection Policy

September 2026

Contents

Introduction 2
Legislative Framework 2
Guidance and Standards 3
Scope and Responsibilities 4
Applicable data 4
Data Protection Principles 5
Accountability 5
Artificial Intelligence (AI) 7
Data protection officer (DPO) 8
Lawful processing 8
Consent 10
The Right to be informed 10
The right of access 11
The Right to Rectification 12
The right to Erasure 13
The Right to Restrict Processing 13
The Right to Data Portability 14
The Right to Object 14
Data Sharing 15
Data protection by design and privacy impact assessments 17
Data Breaches 17
Cyber Security and Cyber Incidents 18
Data Security 20
Safeguarding 24
Publication of Information 24
CCTV and photography 25
Data retention 25
Secure Disposal of Personal Data 26
DBS data 26
Instant Messaging 26
Definitions 28

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
- Freedom of Information Policy
- Photography Policy
- Data and E-security Breach Prevention and Management Plan
- Freedom of Information Policy and Model Publication Scheme
- Surveillance and CCTV Policy
- Child Protection and Safeguarding Policy
- Data Handling Procedures Policy
- Records Management Policy
- AI Policy
- Instant Messaging Policy

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.

Data Protection Principles

We are committed to complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. As such, we ensure that personal data is:

1. **Processed lawfully, fairly and transparently** – We collect and use personal data in a way that is open, clear and in line with the law.
2. **Collected for specified, explicit and legitimate purposes** – We only gather data for clearly defined reasons that support our school's functions and responsibilities.
3. **Adequate, relevant and limited to what is necessary** – We only collect the information we need to fulfil our purpose.
4. **Accurate and, where necessary, kept up to date** – We take steps to ensure information is correct and make updates when appropriate.
5. **Kept for no longer than is necessary** – We retain data only for as long as needed, in line with our retention schedule.
6. **Handled securely** – We use appropriate technical and organisational measures to protect data from unauthorised access, loss or damage.
7. **Accountability** – We take responsibility for our data protection practices and can demonstrate how we comply with these principles.

In accordance with the requirements outlined in the UK GDPR:

- 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.

Record of Processing Activities (RoPA)

In accordance with the principle of accountability, we maintain a comprehensive Record of Processing Activities (RoPA). This record captures important information about the school's data processing activities to improve information governance, demonstrate compliance with accountability principles, and support compliance with other aspects of data protection law, such as creating accurate privacy notices and ensuring data asset security.

Our RoPA includes, as a minimum, the following mandatory information for each processing activity:

- The name and contact details of the school.
- The name and contact details of our Data Protection Officer (DPO).
- The purposes for which personal data is processed.
- The categories of personal data processed.
- The categories of individuals whose personal data is processed.
- The categories of organisations with which personal data is shared.
- The schedule for retaining each category of personal data.
- A general description of our technical and organisational security measures.

Additionally, our RoPA may include further detail such as the source of the personal data, whether the data is Personal Data, Special Category Data, or Criminal Offence Data, the school's role as Data Controller or Data Processor, details of consent obtained, how individuals are informed of their rights, procedures for Subject Access

Requests (SARs), relevant security policies and procedures, secure sharing procedures, data breach handling procedures, and whether the processing involves automated decision-making.

This record is shared with the Senior Leadership Team and Governors, who are responsible for ensuring compliance with the DPA 2018 and that only necessary data is kept.

Artificial Intelligence (AI)

Our school recognises the increasing role of artificial intelligence (AI) in education and administration. While AI tools, particularly Generative AI, can offer significant benefits in education, such as assisting with developing resources like lesson plans, quizzes, communications, or timetables, they also come with considerable data protection risks. It is essential for our school community to understand these risks and how to mitigate them to ensure compliance with data protection legislation.

A key risk with Generative AI models is that information entered into them is generally no longer private or secure. This is because these tools may store, share, or learn from the data you input, including personal or sensitive information, potentially incorporating it into future responses or making it visible to the organisation that owns the tool. For this reason, **staff and pupils must not enter any personal information (personal data, intellectual property, or private information) into any Generative AI model**, especially those classified as 'open' tools which are more accessible and modifiable by external parties. It is not always obvious whether a tool is open or closed, so caution is necessary, and advice should be sought from the Data Protection Officer or IT lead. An example of inappropriate use would be an administrator entering a pupil's name, class, and behavioural details into an open Generative AI tool to draft an email.

Schools should be open and transparent about how they use generative AI tools. Staff should be aware of and inform pupils about the data collection, storage, and usage practices associated with AI technologies, particularly Generative AI. It is important to note that some Generative AI tools may collect and store additional data beyond just the input text, such as location, IP address, system information, and browser information. The data collected by these organisations can potentially be viewed or sold to third parties. Any such data collection, processing, and storage practices by Generative AI tools used by the school must be included in the school's privacy notice.

Staff who wish to utilise AI tools must ensure that the potential new use is assessed to consider if a Data Protection Impact Assessment (DPIA) is required and follow the school's Data Protection Policy and DPIA process. Even signing up to use certain Generative AI models that involve sharing names and email addresses may require a DPIA. An AI-related DPIA will involve considering the nature, scope, context, and purposes of processing personal data, whether individuals expect such processing, available alternatives, and the justification for choosing AI. It will also evaluate whether AI processing and automated decisions may affect individuals, potential individual and allocative harms (including bias), proportionality and fairness, bias or inaccuracy of algorithms, comparison with human accuracy if AI replaces human intervention, how individuals will be informed and can challenge automated decisions, relevant margins of error, the potential impact of security threats, and any planned stakeholder consultations. DPIAs help to identify, measure, and manage data protection risks at an early stage.

The use of AI systems, particularly Generative AI, will be carried out with caution and an awareness of their limitations regarding bias, accuracy, and currency of information. It is crucial to fact-check any results generated by AI tools against reliable sources. The school will take appropriate measures to guarantee the technical robustness and safe functioning of AI technologies, including implementing rigorous cybersecurity protocols and access controls,

establishing oversight procedures, ensuring reporting of security incidents, and evaluating the security of any AI tool before use as part of the DPIA process.

This policy also links to the separate AI Policy and should be read in conjunction with it. Training is also provided to staff on the proper use of AI tools in line with data protection requirements.

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) (or Champion) 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

Under the UK GDPR, all processing of personal data must have a lawful basis. Our school identifies and documents the appropriate legal basis for each processing activity. The lawful bases we rely on include:

1. **Consent** – We may process personal data where the individual has given clear, affirmative consent for us to do so.
2. **Contractual necessity** – We may process personal data when it is necessary to fulfil a contract we have with the individual, or to take steps at the request of the individual before entering into a contract (e.g. processing data for a staff employment contract or a service agreement with parents).
3. **Legal obligation** – We may process personal data when we are required to do so by law (e.g. providing data to the Department for Education, HMRC, or safeguarding agencies).
4. **Vital interests** – In rare circumstances, we may process data to protect someone's life or wellbeing (e.g. in a medical emergency).
5. **Public task (public interest)** – As a public authority, we process personal data where it is necessary for us to carry out our official functions or a task in the public interest (e.g. providing education, safeguarding children, and monitoring attendance).

6. **Legitimate interests** – This basis may apply to activities that are not part of our core public functions but are still necessary for the operation of the school. It requires a balancing test to ensure the individual's rights and freedoms are not overridden (e.g. using CCTV for site security or engaging in limited fundraising activities). This basis is more commonly used by private sector organisations and must be carefully assessed if relied upon.

We ensure that the legal basis for processing is clearly communicated through our privacy notices and documentation, and that data is only processed in accordance with the chosen basis.

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

Special category data is personal data that is more sensitive and therefore requires additional protection.

In a school setting, we may process special category data for purposes such as safeguarding, health and safety, inclusion and wellbeing, or meeting legal obligations.

We are only permitted to process special category data if we meet both:

1. A **lawful basis for processing** under Article 6 of the UK GDPR (as outlined in our Lawful Processing section), **and**
2. An **additional condition under Article 9** of the UK GDPR.

The additional conditions we most commonly rely on include:

- **Explicit consent** – When the data subject has clearly agreed to the processing of their special category data for a specified purpose (e.g. collecting health information for a school trip). Consent must meet the same high standards as outlined in the Lawful Processing section.
- **Employment, social security and social protection law** – For processing necessary to carry out obligations and exercise specific rights in the field of employment or social protection law (e.g. monitoring staff health or managing risk assessments).
- **Vital interests** – When processing is necessary to protect someone's life or wellbeing and the individual is unable to give consent (e.g. a medical emergency).
- **Not-for-profit bodies** – Where the processing is carried out in the course of our legitimate activities as a not-for-profit educational body, provided certain safeguards are in place and the data is not shared outside the organisation without consent.
- **Data made public by the data subject** – Where the individual has deliberately made the data public (e.g. disclosing a medical condition during a public event).
- **Legal claims** – When processing is necessary for the establishment, exercise, or defence of legal claims.
- **Substantial public interest** – Where the processing is necessary for reasons of substantial public interest, based on UK law. This may include safeguarding children and individuals at risk or ensuring equality of opportunity and treatment.
- **Healthcare** – For processing necessary for the provision of health or social care, with appropriate confidentiality safeguards in place.

All processing of special category data is carried out with appropriate safeguards in place, including access controls, staff training, and secure systems, and is limited to what is necessary for the relevant purpose.

Consent

When we rely on consent as a legal basis for processing personal data, it must be:

- **Freely given** – with no pressure or negative consequences for refusal
- **Specific and informed** – clearly explaining what data will be used and why
- **An unambiguous, positive action** – such as ticking a box or signing a form (Silence, inactivity, or pre-ticked boxes do not count as valid consent.)

We keep a clear record of when and how consent was given.

All consent mechanisms we use meet the requirements of the UK GDPR. If valid consent cannot be obtained, we will consider whether another lawful basis applies. If not, the processing will not go ahead.

Consent obtained under the Data Protection Act 1998 will be reviewed to ensure it still meets GDPR standards. Where it does, we will not seek fresh consent.

Individuals have the right to withdraw their consent at any time. We make it easy to do so, and we will stop processing the data as soon as consent is withdrawn.

The Right to be informed

Individuals have the right to be informed about the collection and use of their personal data.

Our privacy notice lets people know what information we have and what we do with it.

It 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 how 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

Handling Subject Access Requests (SARs)

Individuals have the right to access their personal data and supplementary information held by the school. A Subject Access Request (SAR) is the formal process for exercising this right. Requests can be made in writing (email, letter, social media) or verbally (phone, face-to-face) We will treat any request for personal data as a SAR, regardless of how it is phrased, and we do not require requests to be made in a specific format or using a standard form, although a preferred method may be suggested.

Upon receiving a SAR, we will:

- **Acknowledge Receipt:** Record the date the request was received.
- **Verify Identity:** Take reasonable steps to verify the identity of the requester and, if applicable, their authority to act on behalf of another individual (e.g., parental responsibility, legal representation). We may ask for clarification or ID, noting that the data controller decides what alternative ID is appropriate if standard ID cannot be provided. If the requester is a child or representative, we will consider the child's maturity and competence before responding directly to them.
- **Clarify Ambiguous Requests:** If a request is non-specific (e.g., asking for "all information"), we may ask the requester for clarification to help narrow the search, but we cannot require them to reduce their request.
- **Search for Data:** Make reasonable efforts to search through all relevant records where the personal data may be held, including emails (even deleted), documents, databases, CCTV, paper records, and instant messages. Good record keeping and data retention policies facilitate this.
- **Respond within Timeframe:** Respond to all requests without undue delay and **within one calendar month** of receipt. For complex or numerous requests, this period may be extended by up to two additional months, but we will inform the individual in writing within the first month, explaining the delay and the reasons for complexity. **School holidays do not extend the statutory timeframe**.
- **Provide Information:** Provide the requested personal data in a clear, plain language format, typically the same format as the request was received (though a written response is preferable, with a record kept of verbal responses). We will provide information securely, potentially using encryption or secure file transfer methods. We will also include supplementary information as required (purpose of processing, categories of data, recipients, retention period, data subject rights, complaint process).

We may direct requesters to information they already hold or have access to, noting that we hold it but are not re-issuing it.

- **Redact Third-Party Data:** Redact (remove) personal information that identifies other individuals unless their consent is obtained or it is otherwise appropriate on a case-by-case basis. We use appropriate redaction software to ensure redactions cannot be undone, including blurring for CCTV images. Note that a SAR entitles access to one's *own* personal information, not necessarily entire documents containing that information.
- **Handle Unavailable Data:** If requested information is no longer held, we will inform the requester of this, potentially referring to our data retention policy. We may signpost them to another organisation if we know they hold the data.
- **Address Refusals:** We reserve the right to refuse manifestly unfounded or excessive requests, or where a data protection exemption applies (e.g., safeguarding risks, ongoing legal proceedings). If a request is refused or we decide not to take action on a request (e.g., rectification), we will inform the individual of the decision and the reasons, and advise them of their right to complain to the supervisory authority (ICO) and seek judicial remedy within one month.
- **Record Keeping:** Maintain a record of the SAR process from start to finish, including the request date, any pauses, correspondence, records searched, information found, details of redactions and reasons, response details, and evidence of any decisions made (e.g., to refuse or exempt information). This record is crucial for accountability and handling potential complaints or audits.

Requests are handled free of charge, although we may charge for administrative costs if the requester asks for multiple copies. We provide support to individuals who need help making a SAR to ensure accessibility.

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 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.

If 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 several 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 Sharing

We are committed to sharing data securely and appropriately, in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and current statutory guidance.

We may share personal data with third parties where it is lawful, fair, and necessary to do so, including for the purposes of:

- Fulfilling our legal obligations as an education provider
- Safeguarding and promoting the welfare of children
- Supporting learning and pupil development
- Complying with requests from government bodies such as the Department for Education (DfE), Local Authorities, and Ofsted

- Providing services such as IT support, assessment, and school management systems

In accordance with the DfE's guidance and *Keeping Children Safe in Education (2024)*, we recognise that:

"The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children." (KCSIE 2024, para. 119)

Where there is a safeguarding concern, relevant information will be shared with appropriate agencies without delay and without unnecessary concern about data protection barriers. All staff are trained to understand the importance of information sharing in child protection, and follow internal procedures to escalate concerns appropriately.

When sharing data with third parties, we ensure:

- There is a lawful basis for the disclosure
- Only the minimum necessary data is shared
- Information is shared securely
- Records are kept of what data was shared, with whom, and why

We also follow the *Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers* (DfE, July 2018), and any subsequent updates or sector-specific guidance.

Data Processors:

When we rely on the services of several external organisations to support our work (both management and curriculum) these are our "data processors". These include people, companies, systems and software that process personal data as part of the work they do on our behalf. When working with data processors, we carry out appropriate due diligence checks to make sure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to uphold data subjects' rights. We will require contractors and their staff to comply with this Policy.

In accordance with UK GDPR Article 28, we will appoint data processors only on the basis of a legally binding, written contract, that requires them to, amongst other things: only process personal data based on our instructions; keep the data secure; assist us to comply with our legal obligations and uphold data subjects' rights; delete or return the data at the end of the contract; and allow inspections and audits of their processing activities. Data Processor contracts, and compliance, will continue to be monitored throughout the contract period.

We use third-party service providers who may process technical information such as IP address and browser type for operational and security purposes.

Greenhouse for IP address, URL path, User agent and Timestamp. Data is retained for 36 months.

Third Parties:

We will only share personal data with any other external organisation, including other data controllers such as agencies and other schools, when the sharing meets one or more appropriate legal condition, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects. Where necessary we will enter into Data

Sharing Agreements (DSA), or similar agreements, to help facilitate the sharing of personal data. A DSA does not make the sharing lawful, it only provides a framework to work within, to help share data in an effective and safe way that respects people's data protection rights, when an appropriate and lawful reason to share the data has been identified.

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 have considered and integrated data protection into processing activities.

Data Protection Impact Assessments (DPIAs)

In addition to adopting a data protection by design and by default approach, we use Data Protection Impact Assessments (DPIAs) to identify, measure, and manage data protection risks effectively.

A DPIA is required under UK GDPR whenever the processing of personal data is likely to result in a **'high risk to the rights and freedoms'** of individuals. This includes, but is not limited to, systematic and extensive processing activities such as profiling, or large-scale processing of special categories of data or personal data relating to criminal convictions or offences.

An effective DPIA helps us identify and resolve problems at an early stage, minimising risks to individuals' privacy, ensuring expectations are met through privacy notices, demonstrating accountability and compliance, and avoiding reputational damage.

Each DPIA will include:

- A description of the processing operations and their 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 to address and mitigate those risks

If a DPIA indicates high risk data processing that cannot be mitigated, we will consult the Information Commissioner's Office (ICO) to seek their opinion on whether the processing complies with the UK GDPR. We will not begin processing the personal data in question until we have acted on the ICO's advice

DPIAs are not a one-off exercise. They are regularly reviewed and updated if anything changes in our data lifecycle, such as significant changes to how or why we process data, the amount of data collected, the identification of a new security flaw, the availability of new technology, the appointment of a new contractor, or if public concern is raised.

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.

If 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.

If 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, safeguarding our school community, and maintaining operational continuity. In light of updated guidance from the Department for Education (DfE) and the bundled services provided by LGfL, we have adopted a robust approach to cyber security that includes the following measures:

Technical Measures

We implement a range of technical measures to protect our systems and data, including:

- Firewalls, anti-virus software, anti-spam software, URL filtering, secure data backups, encryption, and strong password policies.
- Utilisation of LGfL's **CyberShield** service for real-time threat monitoring and protection against ransomware, phishing attacks, and other cyber threats.
- Deployment of LGfL's **WebScreen** filtering system to ensure compliance with statutory safeguarding guidance (*Keeping Children Safe in Education*). WebScreen provides flexible filtering options based on IP addresses, user groups, or time of day and supports HTTPS decryption for granular filtering.
- Use of LGfL's **MailProtect** email filtering service to protect against email-borne threats such as spam, phishing attempts, viruses, and Denial-of-Service (DoS) attacks. This includes features like multi-layered antivirus scanning, spam digest reports for users, and quarantine management for blocked messages.
- Regular system updates and patch management to address vulnerabilities promptly.

Access Control

We enforce strong access control measures to ensure data security:

- Implementation of multi-factor authentication (MFA) for all users to enhance account security.
- Adherence to the principle of least privilege by regularly reviewing user permissions.

Staff Training

We provide regular cyber security awareness training for all staff, governors, and students. Training covers:

- Recognising phishing attempts and other cyber threats.
- Safe browsing practices.
- Data protection responsibilities.
- Effective use of LGfL services such as CyberShield, WebScreen, and MailProtect.

Incident Response Plan

Our incident response plan outlines clear steps to follow in the event of a cyber attack or breach. It includes:

- Communication protocols for notifying relevant stakeholders.
- Containment strategies to limit the impact of incidents.
- Recovery processes to restore systems and data securely.
- Reporting protocols for serious incidents, including escalation to LGfL's support team or appropriate authorities such as the National Cyber Security Centre (NCSC).

Backup Strategy

We maintain a comprehensive backup strategy in line with best practices:

- At least three backup copies of important data stored on two different media types, with one copy stored off-site.
- Inclusion of cloud-based backups alongside physical backups for added resilience.

Risk Assessments

We conduct regular risk assessments to identify potential vulnerabilities in our systems. Findings are used to update our cyber security measures and improve overall resilience.

Business Continuity Planning

Cyber incidents are explicitly incorporated into our business continuity plans. These plans ensure operational continuity during attacks or outages.

Policy Review

This policy will be reviewed annually or whenever significant updates are issued by the DfE or LGfL. Regular reviews ensure that our approach remains compliant with current standards and leverages available resources effectively.

By prioritising cyber security and leveraging LGfL's bundled services such as CyberShield, WebScreen, MailProtect, and Senso monitoring tools, we aim to protect our school community from the operational, financial, and reputational impacts of cyber incidents. All staff are required to follow this policy and report any suspicious activities or potential breaches immediately.

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

- Personal devices are prohibited from connecting to the school's main wireless network.
- Unauthorised devices pose risks including data breaches and network disruption.
- Violations may result in disciplinary action and will be documented.

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.

- The school will provide training and resources on data protection and network security.

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.

As part of the LGfL service wrap, schools are also provided with a limited number of Egress licences to support secure email and file transfers beyond the USO-FX environment. [Secondary schools 25 licences and primary school 15 licences.] https://lgfl.net/services/egress

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.

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 minimalise 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

Our data protection policy encompasses all safeguarding considerations. All aspects related to data handling in safeguarding contexts are addressed in relevant sections of this policy. We remain committed to ensuring the safety and well-being of our students while adhering to data protection regulations.

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 the 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 Designated Person 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

Our school is committed to adhering to the principles of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), which state that personal data should only be kept for as long as necessary. To ensure compliance, we will undertake an annual review of all personal data held to determine if its retention remains necessary in line with our retention schedule. Any data identified as no longer required will be securely disposed of.

- Personal data will be kept only for as long as it is needed for the purpose for which it was collected
- The retention period for different categories of personal data will be determined based on legal obligations, statutory requirements, contractual necessity, and legitimate school purposes.
- We will maintain a data retention schedule that specifies the retention periods for various types of school records.
- The lawful basis for processing and retaining personal data will be documented.
- We will consider whether data needs to be retained after it has been shared with third parties.
- Where appropriate, we will explore opportunities to depersonalise data for analytical purposes once the primary purpose of retention has been fulfilled.

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

Secure Disposal of Personal Data

Personal data that has reached the end of its retention period will be securely and confidentially disposed of.

Our procedures for data disposal will be clearly defined in this policy, and all staff will be made aware of their responsibilities in adhering to these procedures.

Regular waste streams must not be used for disposing of personal data.

Paper records containing personal data will be shredded using a cross-cutting shredder or by a reputable external company.

Electronic storage media and hard disks will be destroyed to ensure data cannot be retrieved.

When using an external company for data destruction, we will ensure they provide on-site shredding with a staff member present, a certificate of destruction, and evidence of trained staff in handling confidential information.

A record of destroyed data will be maintained, including a brief description, the number of files, and the authorising senior leader, in compliance with the Freedom of Information Act 2000. Shredding will occur promptly after documentation.

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.

Instant Messaging

Our school recognises the use of instant messaging applications for staff communication and has established a dedicated 'Instant Messaging Policy' to ensure this usage aligns with data protection principles and relevant legislation such as the UK-GDPR and the Data Protection Act 2018.

This separate policy provides detailed guidelines on the appropriate use of instant messaging apps when handling personal data, emphasising the need to safeguard personal data and maintain compliance with data protection regulations.

Key data protection considerations addressed within the Instant Messaging Policy include:

- Approved Messaging Apps: Only applications meeting specific security standards are approved for work-related communication to protect personal data. The use of unapproved apps is prohibited.
- Sensitive Information Handling: The policy outlines the need for caution when exchanging sensitive or confidential information, including personal data, and specifies that personal data should only be shared with appropriate security measures, such as encryption, in place.

- Data Encryption: The policy mandates the use of instant messaging apps offering end-to-end encryption for data transmission and restricts the sharing of sensitive information on platforms without this feature.
- Retention and Deletion of Messages: To minimise data retention risks, the policy advises the prompt deletion of messages containing personal data once they are no longer necessary for work-related purposes.
- Data Subject Rights: The Instant Messaging Policy reinforces the need for employees to be aware of and adhere to the school's procedures for responding to data subject rights requests concerning information shared via these apps.
- Access to Personal Devices: In specific circumstances, such as investigating data breaches or responding to data subject requests, the school reserves the right to access personal devices used for work-related communication via approved apps, with clear protocols in place to protect employee privacy and handle data responsibly
- Training and Awareness, Monitoring and Auditing: The school provides training on the proper use of instant messaging apps in line with data protection requirements and may implement monitoring to ensure compliance.

Employees are required to familiarise themselves with and adhere to the guidelines outlined in the Instant Messaging Policy to ensure their use of these communication tools supports the school's commitment to data protection.

Definitions

Definitions used by this school (drawn from the regulations).

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.

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 –

Personal data - Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual

Special categories of personal data Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data.

Personal data relating to criminal offences and convictions is included here for the purposes of this policy.

Data Subject - An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller - The organisation storing and controlling such information (i.e., the School) is referred **to as the Data Controller.**

Processing - Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing - Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA) - DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information - This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

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.

Change Log V15

Edit	Page
Secure file transfer. Egress added as an approved platform.	P19
Data Protection Principles clarified	P05
AI section clarified and explanation added	P06
Legal Bases for Processing – section simplified and clarified	P07
Consent section simplified and clarified.	P09
Data subject rights – minor edits for clarification.	P11
Data sharing updated	P14
Cyber Security and Cyber Incidents updated	P17
Changes to Wi-Fi Access and Security.	P20
Data Retention updated	P24
Secure Disposal of Personal Data added	P24
Instant Messaging added	P25
Definitions updated	P27

Change Log V16

Edit	Page
Record of Processing Activities (RoPA) clarified	P6
Updated AI Section in light of DfE guidance	P7
Enhanced and clarified the right of access	P11
DPIA Section enhanced and clarified	P17

School Development Area Leader: Mrs Caroline Gibbins

Linked Governor: Fiona Hunter

Signed : Fiona Hunter

Signed: Mrs Caroline Gibbins

Date agreed: September 2026

Review date: September 2027