Rutlish School

Data Protection Policy

Committee ownership for this policy: SBC, QoE-Curr, Inclusion, RR6, FGB	SBC
Must be approved by FGB: Y / N	N
Required by:	Statutory
Frequency of review:	Three years
Date last reviewed:	Spring 2026
Date of next review:	Spring 2029
Display on website: Y / N	Y
Responsible	School Business Manager
This policy will be subject to ongoing review and may be amended prior to the scheduled date of next review in order to reflect changes in legislation, where appropriate.	

Contents

INTRODUCTION

This school is committed to being transparent about how it collects and uses data in order to meet its data protection obligations. This policy sets out our commitment to the protection of data.

Please also refer to our HR related policy for specific guidance on the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees.

We may, from time to time, be required to share personal information about employees, students, students or trainees with other organisations, this includes local authorities, Department for Education, other schools and educational bodies, and potentially social services and law enforcement agencies.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how we comply with the principles of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

Organisational methods for keeping data secure are imperative, and we believe that it is good practice to keep clear practical policies, backed up by written procedures.

UK GDPR
The school have signed up to Merton's Data Protection Officer Service Level Agreement. The role of the DPO is to inform and advise us on our data protection obligations.
The DPO can be contacted at schoolsDPO@merton.gov.uk

1. LEGAL FRAMEWORK

This policy meets the requirements set out in the UK GDPR and the DPA 2018. It is based on guidance published by the Information commissioner's Office (ICO) on the UK GDPR.

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018.
- Protection of Freedoms Act 2012 when referring to our use of biometric data; in the act a "young person" means a person under the age of 18.
- Code of practice for the use of surveillance cameras and personal information
- The school Standards and Framework Act 1998
- Privacy and Electronic Communications Regulations (PECR)
- The Environmental Information Regulations 2004

1.1. 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

1.2. 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

1.3. 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)

1.4. Financial and Administrative

- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Public Contracts Regulations 2015 (for procurement record-keeping)
- The Procurement Act 2023

This policy will also have regard to the following guidance:

- Information Commissioner's Office ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- Department for Education (2018) 'Data Protection: A toolkit for schools'

2. 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
- CCTV Policy
- Safeguarding and Child Protection Policy
- Data Handling Procedures Policy
- Records Management Policy
- AI Policy

3. THE DATA CONTROLLER

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school pays a fee to register with the ICO as legally required.

4. ROLES AND RESPONSIBILITIES

This policy applies to **all staff,** including temporary staff**,** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1. Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.2. Data Protection Officer

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.
The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.
Our DPO is London Borough of Merton and is contactable via schoolsDPO@merton.gov.uk.

However, our **data protection lead** has day-to-day responsibility for data protection issues in our school. If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact them: School Business Manager (SBM) email administration@rutlish.merton.sch.uk

4.3. School Business Manager

The SBM acts as the representative of the data controller on a day-to-day basis.

4.4. All staff

Staff are responsible for:

a) Collecting, storing and processing any personal data in accordance with this policy
b) Informing the school of any changes to their personal data, such as a change of address
c) Contacting the DPO in the following circumstances:
   - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
   - If they have any concerns that this policy is not being followed
   - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
   - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
   - If there has been a data breach
   - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
   - If they need help with any contracts or sharing personal data with third parties

5. 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'**, These specifically include the processing of race; ethnic origin; politics; religion; trade union membership; genetics; biometrics where used for ID purposes); health; sex life; or sexual orientation.

6. PRINCIPLES

In accordance with the requirements outlined in the UK GDPR, personal data will be:

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

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with these principles".

7. 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 and EU refer to the ICO guidance, 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.

8. 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.

9. 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 students 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 student'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 students 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.

10. LAWFUL PROCESSING

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
b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
c) Processing is necessary for compliance with a legal obligation
d) Processing is necessary to protect the vital interests of an individual or another person
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
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

In order to lawfully process special category data, we will identify both a lawful basis under Article 6 above and a separate condition for processing special category data under Article 9 below.

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

a) The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
b) The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
c) The data has already been made **manifestly public** by the individual
d) The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
e) The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

11. LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

12. SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

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.

13. 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 requested to be withdrawn by an individual at any time.

14. 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 young person, we will ensure that the privacy notice is written in a clear, plain manner that the young person 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.

15. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

15.1. Subject assess request

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Where a SAR has been made for information held about a young person, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the young person can understand their rights, it will respond directly to the young person.

We will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

We will 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.

Where a request is manifestly unfounded or excessive, we hold the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, we will ask the individual to specify the information the request is in relation to.

a) How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
b) The right to lodge a complaint with the ICO or another supervisory authority.
c) The source of the data, if not the individual.
d) Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
e) The safeguards provided if the data is being transferred internationally.

We will 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.

If staff receive a subject access request in any form, they must immediately forward it to the DPO (School Business Manager).

15.2. Young people and subject access requests

Personal data about a young person belongs to that young person, and not the young person's parents or carers. For a parent or carer to make a subject access request with respect to their young person, the young person must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Young people aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Parents, or those with parental responsibility, have a legal right to free access to their young person's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

16. RESPONDING TO SUBJECT ACCESS REQUESTS

a) When responding to requests, we:
b) May ask the individual to provide two forms of identification
c) May contact the individual via phone to confirm the request was made
d) Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
e) Will provide the information free of charge
f) May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

a) Might cause serious harm to the physical or mental health of the student or another individual

b) Would reveal that the young person is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the young person's best interests
c) Would include another person's personal data that we can't reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
d) Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
e) If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.
f) When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

17. OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

a) Withdraw their consent to processing at any time
b) Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
c) Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
d) Be notified of a data breach (in certain circumstances)
e) Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.
Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible.
Where appropriate, we will inform the individual about the third parties that the data has been disclosed to.
Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
Where no action is being taken in response to a request for rectification, we will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to 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 defense 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 student 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 defense 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 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.

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.

18. BIOMETRIC RECOGNITION SYSTEMS

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their young person first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data

from their young person. In no circumstances can a young person's biometric data be processed without written consent and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). The school must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

What does processing data mean?
'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a) Recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
b) Storing students' biometric information on a database system; or
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise students.

19. 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 Retention Schedule.

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. The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school device containing non-encrypted personal data about students

20. 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.

21. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Confidential paper records are kept in locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up.

Where data is saved on removable storage or a portable device, this device will be encrypted using Advanced Encryption Standard (AES) 256-Bit Security to FIPS-197 standard. Such devices will be kept in a locked filing cabinet, drawer or safe when not in use. Where possible, we enable electronic devices to allow the remote blocking or deletion of data in case of theft or loss. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded that they should not share passwords.

Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use agreement).

Staff and governors will not use personal email accounts or personal cloud storage for school business.

Members of staff who access the school network are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Remote access to school systems is permitted based on a credible business case. When permission is granted remote access will be via LGFL CISCO anywhere client. Use of second factor authentication is mandatory for remote access to the school network. This includes the use of both 'soft' and 'hard' One Time Passwords.

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

Wi-Fi access to the school network is permitted from school devices. All school devices use WPA3 encryption for Wi-Fi connections. Staff owned devices and visitors must use the separate Guest Wi-Fi.

Access to files on the school network is on a need to know basis - files and folders have granular permissions base on staff seniority and role. File access is monitored and reviewed. We actively monitor Wi-Fi usage for unusual activities or potential security threats.

Email is not a secure medium for external communication and should be used as a last resort for sending sensitive or confidential information. If documents are sent by email they should be encrypted with a password. This school uses the Secure Document Transfer Portal (USO-FX) provided by the LGFL to transfer information securely.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

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 we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

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

Visitors to areas containing sensitive information will be supervised at all times.

The physical security of our buildings and storage systems, and access to them, is reviewed on annually. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

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

The Data Protection Officer will assist in making sure that continuity and recovery measures are in place to ensure the security of protected 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 student 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.

22. 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.

23. 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.

24. CCTV AND PHOTOGRAPHY

We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with the ICO's code of practice for the use of CCTV. We use CCTV in various locations around the school site to ensure it remains safe.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system please contact us (see 'Contact us' below). 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 one months for security purposes; the Designated Person is responsible for keeping the records secure and allowing access.

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are exempt from the UK GDPR. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

When using photographs and videos in this way we will not accompany them with any other personal information about the young person, to ensure they cannot be identified.

25. 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 *(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)*

Unrequired data will be deleted as soon as practicable. Some educational records relating to former students or employees 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.

Where appropriate, we will explore opportunities to depersonalise data for analytical purposes once the primary purpose of retention has been fulfilled.

26. 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.

27. 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.

28. TRAINING

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

29. 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) – the UK GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to

controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

Article 4 definitions.

Establishment – the main establishment of the controller in the UK will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – 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 – 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.

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

Data controller – A person or organisation that determines the purposes and the means of processing of personal data.

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.

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.

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.

Young person – the UK GDPR defines a young person as anyone under the age of 16 years old. The processing of personal data of a young person 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 young person.

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 (CPO) – person responsible for implementing and developing data protection as communicated by the DPO.

APPENDIX 1

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

a) On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email.

b) The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
   a. Lost
   b. Stolen
   c. Destroyed
   d. Altered
   e. Disclosed or made available where it should not have been
   f. Made available to unauthorised people

c) Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

d) If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher and the chair of governors.

e) The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure).

f) The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

g) The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

h) The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on GDPRiS online system and the school network securely, paper copies are stored in locked a cupboard with minimum access.

i) Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
   a. A description of the nature of the personal data breach including, where possible:
      i. The categories and approximate number of individuals concerned.
      ii. The categories and approximate number of personal data records concerned.
   b. The name and contact details of the DPO.
   c. A description of the likely consequences of the personal data breach.
   d. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

j) If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

k) Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
   a. A description, in clear and plain language, of the nature of the personal data breach.
   b. The name and contact details of the DPO.
   c. A description of the likely consequences of the personal data breach.
   d. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

l) The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

m) The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
   a. Facts and cause

b. Effects
c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

n) Records of all breaches will be stored on GDRPiS.
o) The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
p) The DPO and Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

a) If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Technicians to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
b) Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
c) In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
d) The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
e) The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

PRIVACY NOTICE – Secondary Schools Students Parents/Carers

HOW WE USE YOUR INFORMATION

Introduction
This notice is to help parents understand how and why Rutlish School collects your child's personal information and what we do with that information. It also explains the rights you have in relation to your child's information.

We are giving you this notice because you are able to exercise your child's data protection rights on their behalf. When your child is older (usually when they reach the age of 13) they will be considered mature enough to exercise their own data protection rights.

Our Data Protection Officer/Lead is the School Business Manager (see 'Contact us' below).

If you have any questions about this notice please talk to the Head of Year.

What is "personal Information"?
Personal information is information that the school holds about your child and which identifies your child.

This includes information such as their date of birth and address as well as things like exam results, medical details and behaviour records. The school may also record your child's religion or ethnic group. CCTV, photos and video recordings of your child are also personal information.

The categories of student information that we process include:
- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- Free school meal entitlement
- Identity management/authentication (to log into school systems)

Why does the school collect and use personal information?
We collect and use student information, for the following purposes:
a) to support student learning
b) to monitor and report on student attainment progress
c) to provide appropriate pastoral care
d) to execute our safeguarding responsibilities
e) to assess the quality of our services
f) to keep children safe (food allergies, or emergency contact details)
g) to meet the duties placed upon us for the Department for Education (DfE) data collections
h) to support our local authority with planning future provision

We set out below examples of the different ways in which we use personal information and where this personal information comes from. Our primary reason for using your child's information is to provide your child with an education.

The admissions forms which you complete give us personal information about your child. We get information from your child, their teachers and other students. Your child's previous school also gives us information about your child if we need this to teach and care for them.
Sometimes we get information from your child's doctor and other professionals where we need this to look after your child.

We collect this information to help the School run properly, safely and to let others know what we do here. Here are some examples:

- We need to tell all appropriate members of staff if your child is allergic to something or might need extra help with some tasks.
- We may need to share information about your child's health and wellbeing with the School Nurse or counsellor.
- We may use CCTV to make sure the school sites are safe. CCTV is not used in private areas such as changing rooms. CCTV policy is available on request.
- We may need to report some of your child's information to the government. For example, we may need to tell the local authority that your child attends our school or let them know if we have any concerns about your child's welfare.
- We may need information about any court orders or criminal petitions which relate to your child. This is so that we can safeguard your child's welfare and wellbeing and the other students at the school.
- If your child is from another country, we have to make sure that they have the right to study in the UK. We might have to provide their information to UK Visas and Immigration.
- Depending on where your child will go when they leave us we may need to provide their information to other schools. For example, we may share information about your child's results and provide references. We may need to pass on information, which they need to look after your child.
- We may need to share information with the police or our legal advisers if something goes wrong or to help with an inquiry. For example, if one of your child's classmates is injured at school or if there is a burglary.
- Occasionally we may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the school properly. We might need to share your child's information with them if this is relevant to their work.
- If your child has misbehaved in a serious way, and the police have become involved, we may need to use information about the action taken by the police.
- We may share some information with our insurance company to make sure that we have the insurance cover that we need.
- We may share your child's academic and (where fair) their behaviour records with you or their education guardian so you can support their schooling.
- We will only share your child's information with other people and organisations when we have a good reason to do so. In exceptional circumstances, we may need to share it more widely than we would normally.
- We will monitor your child's use of email, the internet and mobile electronic devices e.g. iPads. This is to check that your child is not misbehaving when using this technology or putting themselves at risk of harm. If you would like more information about this you can read the acceptable use of IT and email policy or speak to your child's class teacher.
- We employ a system that decrypts and inspects HTTPS web traffic within our network to enhance online safety and ensure compliance with safeguarding regulations. This process helps prevent access to harmful content and maintains a secure online learning environment. Personal identifiers and usage data are processed for this purpose, and data security measures are rigorously maintained.
- We may use photographs or videos of your child for our websites and social media sites or prospectus to show prospective students what we do here and to advertise the school. We may continue to use these photographs and videos after your child has left the school.
- Sometimes we use photographs and videos for teaching purposes, for example, to record a drama lesson. If you have any concerns about us using photographs or videos of your child please speak to your child's class teacher.
- We publish our public exam results, sports fixtures and other news on the website and put articles and photographs in the local news to tell people about what we have been doing.
- We sometimes use contractors to handle personal information on our behalf. The following are examples:
  - IT consultants who might access information about your child when checking the security of our IT network; and
  - We use third party "cloud computing" services to store some information rather than the information being stored on hard drives located on the school site.

If you have any concerns about the above, please speak to child's Head of Year.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing student information are:

Public interest
This means that the processing of your child's data is necessary for public interest. The school relies on public interest for most of the ways in which it uses your child's information.
Specifically, the School has a public interest in:

- Providing your child with an education.
- Safeguarding and promoting your child's welfare and the welfare of other children.
- Promoting the objectives and interests of the school.
- Facilitating the efficient operation of the school.
- Ensuring that all relevant legal obligations of the school are complied with.

If you object to us using your child's information where we are relying on our public interests as explained above, please speak to Head of Year.

Legal obligation
Where the School needs to use your child's information in order to comply with a legal obligation, for example to report a concern about your child's wellbeing to Children's Services, we may also have to disclose your child's information to third parties such as the courts, the local authority or the police where legally obliged to do so.

Legitimate interest
Personal data may be processed on the basis that the school has a legitimate interest in processing that data, provided that such legitimate interest is not overridden by the rights or freedoms of the child.

The school must also comply with an additional condition where it processes special categories of personal information. These special categories include: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, and information about sex life or orientation.

Vital interests
To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal claims
The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Consent
We may ask for your consent to use your child's information in certain ways. If we ask for your consent to use your child's personal information you can take back this consent at any time. Any use of your child's information before you withdraw your consent remains valid. Please speak to your child's Head of Year if you would like to withdraw any consent given.

Sharing Under Recognised Legitimate Interest — DUAA 2025
Under the Data Use and Access Act (DUAA) 2025, we may share personal information when we have a good reason that doesn't take away your rights. Before we do this, we will:

- Identify the specific reason for sharing.
- Check that sharing is necessary and fair.
- Complete a Legitimate Interest Assessment (LIA) and put in place protections, like limiting access to the data.

We will keep records of the reasons for sharing, the types of data shared, and who it is shared with. You have the right to object to this sharing.

Collecting student information
The admissions forms which you complete give us personal information about your child. We get information from your child, their teachers and other students. Your child's previous school also gives us information about your child if we need this to teach and care for them.
Sometimes we get information from your child's doctor and other professionals where we need this to look after your child.

Student data is essential for the school's operational use. Whilst the majority of student information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data
We keep your child's information for as long as we need to in order to educate and look after them. We will keep certain information after your child has left school.

In exceptional circumstances, we may keep your child's information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under data protection law.

We hold student data securely for the set amount of time shown in our data retention schedule. Please contact the school office for more information on our data retention schedule and how we keep your data safe.

Who do we share student information with?
We routinely share student information with:
- Schools that the students attend after leaving us
- The NHS
- Public Health England
- School Nurse Team
- The Department for Education (DfE).
- Our local authority London Borough of Merton. We are required to share information about our students with our local authority under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013, such as safeguarding concerns and information about exclusions.
- Our regulator, Ofsted.
- Suppliers and service providers: to be able to provide a service to the students eg. exam centres, catering services, youth support service provider, trip and residential companies this is not limited to.
- Financial organisations to fund services that are not provided by the school.
- Health authorities to meet our legal obligations, e.g. if you had an accident at school.
- Security organisations to use the biometrics system or access to the school gates.
- Health and social welfare organisations to ensure your wellbeing.
- Professional advisers and consultants to seek advice to support you in your education.
- Charities and voluntary organisations to be part of the PTA.
- Police forces, courts, the school may need to share information to these services.

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

Merton Family Hub
Students aged 11+
Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth services as they have responsibilities in relation to the education or training of 11–19-year-olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:
- youth services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / student once they reach the age 16.

Data is securely transferred to the Merton Family Hub via Egress and is stored securely on CPOMS and held for minimum of DOB +25 years but case specific.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth services as they have responsibilities in relation to the education or training of 11–19-year-olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth services
- careers advisers

Data is securely transferred to the Merton Family Hub via Egress and is stored securely on CPOMS and held for minimum of DOB +25 years but case specific.
For more information about services for young people, please visit our local authority website.

Department for Education (DfE)
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our students with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

- section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section. For privacy information on the data the Department for Education collects and uses, please see: https://www.gov.uk/government/publications/privacy-information-early-years-foundation-stage-to-key-stage-3
and
https://www.gov.uk/government/publications/privacy-information-key-stage-4-and-5-and-adult-education

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data
The UK-GDPR gives parents and students certain rights about how their information is collected and used. To make a request for your personal information, or be given access to your child's educational record, contact School Office. Adminstration@rutlish.merton.sch.uk

You also have the following rights:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of your personal information we have about you – this is called 'right of access', this is also known as a subject access request (SAR), data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at raise a concern with ICO.

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint
Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the School Business Manager administration@rutlish.merton.sch.uk

Last updated
We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on Spring 2026.

Contact
If you would like to discuss anything in this privacy notice, please contact: The School Business Manager administration@rutlish.merton.sch.uk.

How Government uses your data
The student data that we lawfully share with the Department for Education (DfE) through data collections:
- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Student Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements
To find out more about the data collection requirements placed on us by the Department for Education (DfE) (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education (DfE) and contains information about students in schools in England. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
The data in the NPD is provided as part of the operation of the education system and is used for research and statistical purposes to improve, and promote, the education and well-being of children in England.
The evidence and data provide DfE, education providers, Parliament and the wider public with a clear picture of how the education and children's services sectors are working in order to better target, and evaluate, policy interventions to help ensure all children are kept safe from harm and receive the best possible education.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-npd-privacy-notice/national-pupil-database-npd-privacy-notice

Sharing by the Department for Education (DfE)
DfE will only share students' personal data where it is lawful, secure and ethical to do so. Where these conditions are met, the law allows the Department for Education (DfE) to share students' personal data with certain third parties, including:
- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department for Education's (DfE) NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department for Education (DfE) has provided student information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

How to find out what personal information the Department for Education (DfE) holds about you
Under the terms of the UK GDPR, you are entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:
https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter
or
https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights
To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Use of your persona data for marketing purposes
Where you have given us consent to do so, we may send you marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by clicking on the 'Unsubscribe' link at the bottom of any such communication, or by contacting us (see 'Contact us' below).

Use of your personal data in automated decision making and profiling
We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Transferring data internationally
We may share personal information about you with the following international third parties outside of the European Economic Area, where different data protection legislation applies:

- To universities and schools, the school will transfer data on the basis of an adequacy decision by the European Commission.
- We may store your information on cloud computer storage based overseas or communicate with you by email when you are overseas (for example, when you are on holiday).

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law.

The European Commission has produced a list of countries which have adequate data protection rules. The list can be found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

If the country that we are sending your information to is not on the list or, is not a country within the EEA (which means the European Union, Liechtenstein, Norway and Iceland) then, it might not have the same level of protection for personal information as there is the UK.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

APPENDIX 3

RUTLISH SCHOOL

PRIVACY NOTICE – Students 13-18

HOW WE USE YOUR INFORMATION

Introduction

This notice is provided to help you (the student) understand how and why Rutlish School collects your personal information and what the school does with that information.

Because you are usually considered mature enough when you reach the age of 13, you are now able to exercise your own data protection rights.
If you have any questions about this notice, please talk to the Head of Year.

What is "personal information"?

Personal information is any information the School holds about you that identifies you. This includes factual details and records:

- Identifiers and Contacts (such as your name, unique pupil number, contact details, and address).
- Characteristics (such as ethnicity, language, and free school meal eligibility).
- Records (like exam results, behaviour records, and attendance data).
- Sensitive Data (such as medical details, religion, or ethnic group).
- Safeguarding information (such as court orders and professional involvement).
- Media (CCTV, photos, and video recordings of you).

Why the School Collects and Uses Your Information

The primary reason the school uses your information is to provide you with an education. We collect and use your data for several key purposes:

- To support your learning and monitor your attainment progress.
- To provide appropriate pastoral care and execute the school's safeguarding responsibilities.
- To keep you safe (e.g., managing food allergies or using emergency contact details)
- To comply with duties placed upon the school for Department for Education (DfE) data collections.

We sometimes need to share your information to make sure the school runs properly and safely. For example:

- We must tell appropriate staff if you are allergic to something or need extra help with tasks.
- We may share information about your health and wellbeing with the School Nurse or counsellor.
- We use CCTV on school sites (but not in private areas like changing rooms) to ensure safety.
- We may have to provide your information to UK Visas and Immigration if you are from another country and we must verify your right to study in the UK.
- Sharing Your Information (Especially Relevant for 13+)

The school will only share your information with others when there is a good reason to do so, or when legally required.

Merton Family Hub
Youth Support Services (Age 13+):

Once you reach the age of 13, we are required under section 507B of the Education Act 1996 to share certain details with our local authority and/or provider of youth support services. This sharing helps them provide services like youth support services and careers advisers.

- The mandatory information shared is limited to your name, address, and date of birth.
- Currently, if your parent or guardian provides their consent, other information relevant to youth support services will be shared; however, this right to provide consent will be transferred to you once you reach the age of 16.

We routinely share student information with other entities as well, including schools you attend after leaving us, the NHS, Public Health England, the School Nurse Team, the Department for Education (DfE), and our local authority.

We also monitor your use of IT:

- We will monitor your use of email, the internet, and mobile electronic devices (e.g., PC, laptops) to check that you are not misbehaving or putting yourself at risk of harm.
- We employ a system that decrypts and inspects HTTPS web traffic within our network to enhance online safety and prevent access to harmful content.

Your Data Protection Rights (Under UK GDPR)
As a student over 13, you are generally able to exercise your own data protection rights. You can make a request for your personal information, or access your educational record, by contacting The School Business Manager.

You have the following rights concerning your personal data:
- Right to be informed about how your data is collected and used.
- Right of access (or Subject Access Request - SAR) to ask us for copies of the personal information we hold about you.
- Right to rectification to ask us to change any information you think is not accurate or complete.
- Right to erasure to ask us to delete your personal information (though this right does not apply when the lawful basis for processing is a legal obligation or public task).
- Right to object to processing of your information, in certain circumstances (though this right does not apply if we rely on legal obligation or vital interests).
- Right to withdraw consent at any time if we are relying on your consent for processing.

If we ask for your consent to use your personal information, you can take back this consent at any time.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office (ICO).

APPENDIX 4

RUTLISH SCHOOL

PRIVACY NOTICE – Students Over 18

HOW WE USE YOUR INFORMATION

Introduction

This notice is provided to help you (the student, who is over 18) understand how and why Rutlish School collects your personal information and what the school does with that information.

As you are over 18, you are fully recognised as the data subject and rights holder regarding your personal information. If you have any questions about this notice, please talk to the Head of Year.

What is "personal information"?

Personal information is any information the School holds about you that identifies you. This includes factual details and records:

- Identifiers and Contacts (such as your name, unique pupil number, contact details, and address).
- Characteristics (such as ethnicity, language, and free school meal eligibility).
- Records (like exam results, behaviour records, and attendance data).
- Sensitive Data (such as medical details, religion, or ethnic group).
- Safeguarding information (such as court orders and professional involvement).
- Media (CCTV, photos, and video recordings of you).

Why the School Collects and Uses Your Information

The primary reason the school uses your information is to provide you with an education.
We collect and use your data for several key purposes:

- To support your learning and monitor your attainment progress.
- To provide appropriate pastoral care and execute the school's safeguarding responsibilities.
- To keep you safe (e.g., managing food allergies or using emergency contact details)
- To comply with duties placed upon the school for Department for Education (DfE) data collections.
- To assess the quality of the services provided by the school.

We gather information from various sources, including admissions forms, your previous schools, your teachers and other staff, and sometimes from doctors or other professionals where necessary for your care.

Sharing Your Information

The school will only share your information with others when there is a good reason or when legally required.
We routinely share your information with:

- Schools that you attend after leaving us, including information about results and references.
- The NHS, Public Health England, and the School Nurse Team.
- Our local authority (as required under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013).
- The Department for Education (DfE) either directly or via the local authority for statutory data collections.

Merton Family Hub

Youth Support Services (Age 16 to 19):

Because the local authority and youth support services have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996, we share certain information with them, which enables them to provide services such as:

- Post-16 education and training providers.
- Youth support services.
- Careers advisers.

The mandatory information shared is limited to your name, address, and date of birth. As you are over 16, the right to consent to the sharing of other information relevant to youth support services rests entirely with you.

Other Sharing and Monitoring:

- We may share information with UK Visas and Immigration if you are from another country and we must verify your right to study in the UK.
- We may share information with the police or our legal advisers if something goes wrong or to help with an inquiry.
- We use CCTV on school sites (but not in private areas like changing rooms) to ensure safety.
- We will monitor your use of email, the internet, and mobile electronic devices (e.g., PC, laptops) to check that you are not misbehaving or putting yourself at risk of harm.
- We employ a system that decrypts and inspects HTTPS web traffic within our network to enhance online safety, ensure compliance with safeguarding regulations, and prevent access to harmful content.

Lawful Bases for Processing Your Data

The UK General Data Protection Regulation (UK GDPR) requires us to have a lawful basis for processing your information. The primary bases we rely on are:

1. **Public Interest:** The processing of your data is necessary for public interest, which includes providing you with an education, safeguarding your welfare, and promoting the objectives and efficient operation of the school. If you object to processing based on public interest, you should speak to the Headteacher.
2. **Legal Obligation:** We must use your information to comply with legal requirements, such as reporting concerns about wellbeing to Children's Services or disclosing information to the courts, the local authority, or the police when legally obliged.
3. **Legitimate Interest**: We may process data if the school has a legitimate interest, provided that your rights or freedoms are not overridden.
4. **Vital Interests**: To protect the vital interests of any person where consent cannot be given (e.g., if you are seriously hurt and unconscious).
5. **Legal Claims**: Processing is necessary for the establishment, exercise, or defence of legal claims (allowing us to share information with legal advisors and insurers).
6. **Consent**: If we rely on your consent to use your information in certain ways, you can withdraw this consent at any time.

Your Data Protection Rights (Under UK GDPR)

As an adult student (over 18), you are fully entitled to exercise your own data protection rights:

Right	Description	Key Detail
Right to be informed	To be informed about how your data is collected and used.	
Right of Access (SAR)	To ask us for copies of the personal information we hold about you.	
Right to Rectification	To ask us to change any information you think is not accurate or complete.	
Right to Erasure	To ask us to delete your personal information.	This right does not apply when the lawful basis is legal obligation or public task.
Right to Restriction	To ask us to stop using your information in certain ways.	
Right to Object to Processing	To object to the processing of your information, in certain circumstances.	This right does not apply if we rely on legal obligation, contract, or vital interests.
Right to Withdraw Consent	To withdraw consent at any time where we rely on your consent for processing.	

To make a Subject Access Request (SAR) or access your educational record, contact The School Business Manager.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office (ICO).

HOW WE USE YOUR INFORMATION

Introduction

Under UK data protection law, individuals have a right to be informed about how our school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage to work at our school.

We, Rutlish School, Watery Lane, SW20 9AD, 020 8542 1212 are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer/Lead is the School Business Manager (see 'Contact us' below).

The categories of information that we process include

We process data relating to those we employ, or otherwise engage, to work within our School.
Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process.
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving license
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences. We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we collect and use workforce information We use the data listed above to:
The purpose of processing this data is to help us run the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Support effective performance management
- Inform our recruitment and retention policies

- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

We only collect and use personal information about you when the law allows us to. Under the General Data Protection Regulation (GDPR)Articles 6 and 9, the legal basis / bases we rely on for processing personal information for general purposes are:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data – for example, where we need to investigate a matter of serious misconduct.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting workforce information

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with data protection regulations, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

Personal data is stored in line with our data protection policy.

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our data protection policy and retention schedule. Our retention guidelines are informed by the Information and Records Management Society's toolkit for schools.

Who we share workforce information with and why

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Sharing under recognised legitimate interest — DUAA 2025

Under the Digital Services Act (DUAA) 2025, we may in limited circumstances share personal data where we have a recognised legitimate interest and that interest is not overridden by the rights and freedoms of the individual. Before relying on this basis we will identify the specific legitimate interest, assess and document why the processing is necessary and proportionate, complete a Legitimate Interest Assessment (LIA), and put in place safeguards (for example, data minimisation, pseudonymisation where possible, contractual protections and restricted access). If we rely on this basis we will record the interest, the categories of data and recipients, and explain how you can object. Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- The Department for Education to comply with a legal obligation
- Your family or representatives to carry out a task in the public interest
- Educators and examining bodies to carry out a task in the public interest

- Ofsted to carry out a task in the public interest
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll, HR and budgeting
- Financial organisations to comply with a legal obligation
- Our auditors to comply with a legal obligation
- Survey and research organisations to carry out a task in the public interest
- Trade unions and associations to comply with a legal obligation
- Health authorities to carry out a task in the public interest
- Security organisations to comply with a legal obligation
- Health and social welfare organisations to carry out a task in the public interest
- Professional advisers and consultants to comply with a legal obligation
- Charities and voluntary organisations to carry out a task in the public interest
- Police forces, courts, tribunals to comply with a legal obligation
- Professional bodies to comply with a legal obligation
- Employment and recruitment agencies to comply with a legal obligation

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.
We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
We are required to pass information about our child and family social work workforce employees to the Department for Education (DfE) through regulations under Section 83 of the Children Act 1989.
All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.
For more information, please see 'How Government uses your data' section.
For privacy information on the data the Department for Education (DfE) collects and uses, please see:
https://www.gov.uk/government/publications/privacy-information-education-providers-workforce-including-teachers.

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the School Business Manager.

You also have the following rights:
- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request, data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:
- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.

- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint
Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know.
We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact The School Business Manager.

Alternatively, you can make a complaint to the Information Commissioner's Office:
- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Last updated
We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on Spring 2026.

Contact
If you would like to discuss anything in this privacy notice, please contact: School Business Manager email administration@rutlish.merton.sch.uk.

How Government uses your data
The workforce data that we lawfully share with the Department for Education (DfE) through data collections:
- informs the Department for Education (DfE) policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements
To find out more about the data collection requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department for Education (DfE)
The Department for Education (DfE) may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:
- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department for Education (DfE) will only share your personal data where it is lawful, secure and ethical to do so and has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the Department for Education (DfE) releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of public benefit, proportionality, legal underpinning and strict information security standards.

For more information about the Department for Education's (DfE) data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the Department for Education (DfE) has provided information, (and for which project) please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

How to find out what personal information the Department for Education (DfE) hold about you
Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:
https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter
or
https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Use of your personal data for marketing purposes
Where you have given us consent to do so, we may send you marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by clicking on the 'Unsubscribe' link at the bottom of any such communication, or by contacting us (see 'Contact us' below).

Use of your personal data in automated decision making and profiling
We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Transferring data internationally
We may share personal information about you with the following international third parties outside of the European Economic Area, where different data protection law applies:

- To reference to other countries, the school will transfer data on the basis of an adequacy decision by the European Commission.

Where we transfer your personal data to a country or territory outside the European Economic Area, we will follow data protection law.

In cases where we have safeguarding arrangements in place, you can get a copy of these arrangements by contacting us.

APPENDIX 6

RUTLISH SCHOOL

PRIVACY NOTICE – Governors and other volunteers

Introduction

This privacy notice has been written to inform governors, and volunteers about how and why we process your personal data.

Rutlish School is a data controller as defined by the UK GDPR. This means that we determine the purposes for which your personal data is processed and the manner of the processing. We will only collect and use your personal data in ways that are compliant with data protection legislation.

The school has appointed London Borough of Merton as its Data Protection Officer (DPO). The role of the DPO is to monitor our compliance with the UK GDPR and the Data Protection Act 2018 and advise on data protection issues.

What personal information do we collect?

The personal data we collect about you includes:

- Personal identifiers, including your name, address and contact details.
- Information relating to your particular role, i.e. if you are a parent governor, community governor etc.
- Information about the history of your appointment.
- Your business and/or financial interests, where applicable.
- Relevant criminal history data, including your DBS check, where applicable.
- Photographs or video images of you, including CCTV footage.
- Relevant skills, expertise and qualifications.
- References you have provided.
- Records of communications and interactions we have with you.
- Equality monitoring information, such as your ethnicity, religious beliefs and gender.
- Information about any health condition or disability you may disclose.
- E-monitoring information about your use of the school's network and IT systems.

Why do we collect your personal information?

The personal data collected is essential, in order for the school to fulfil their official functions and meet legal requirements.

We process your information for the purposes outlined below:

- To meet the statutory duties placed upon us
- To establish and maintain effective governance.
- To meet our safeguarding obligation to students and the school workforce.
- To meet statutory obligations for publishing and sharing governor or trustee details.
- To meet our health and safety obligations.
- To monitor and manage skills, training and personal development.
- To make any reasonable adjustments you may need in relation to a health condition or disability.
- To promote the school, including in newsletters, on the school website and social media platforms.

What is our lawful basis for processing your information?

Under the UK General Data Protection Regulation (GDPR) 2018

, the legal bases we rely on for processing personal information for general purposes are:

- Article 6(1)(c) - legal obligation
- Article 6(1)(e) - public task

There may be occasions where our processing is not covered by one of the legal bases above. In that case, we may rely on Article 6(1)(f) - legitimate interests. We only rely on legitimate interests when we are using your data in ways you would reasonably expect.

All local authority-maintained school governing bodies, under section 538 of the Education Act 1996 have a legal duty to provide the governance information as detailed above.

For the processing of personal data relating to criminal convictions and offences, processing meets Schedule 1, Part 2 of the Data Protection Act 2018 as below:

- (10) Preventing or detecting unlawful acts

Some of the information we collect about you is classed as special category data under the UK GDPR. The additional conditions that allow for processing this data are:

- Article 9(2)(g) - reasons of substantial public interest

The applicable substantial public interest conditions in Schedule 1 of the Data Protection Act 2018 are:

- Condition 6 - statutory and government purposes
- Condition 10 - preventing or detecting unlawful acts
- Condition 18 - safeguarding of children and vulnerable people

Sharing under Recognised Legitimate Interest — DUAA 2025
Under the Data Use and Access Act (DUAA) 2025, we may share personal data when we have a recognised legitimate interest that does not override individual rights and freedoms. Before doing so, we will:

- Identify the specific legitimate interest.
- Assess and document the necessity and proportionality of the processing.
- Complete a Legitimate Interest Assessment (LIA) and implement safeguards, such as data minimization and restricted access.

We will maintain records of the legitimate interest, categories of data shared, and recipients. You have the right to object to this processing.

Who do we obtain your information from?
We normally receive this information directly from you, for example via documents and other records and information supplied by you in the course of your application for the role or a period of volunteering. However, we may also receive some information from the following third parties:

- Disclosure and Barring Service (DBS).
- Local Authority.
- Referees you have provided.
- Governor support services, if applicable.

Who do we share your personal data with?
We may share your information with the following organisations:

- Department for Education (DfE), Government departments or agencies (Health authorities)
- Disclosure and Barring Service (DBS).
- Local Authority - to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Any relevant funding authority.
- Our IT application providers, where relevant to your role.
- Our regulator, Ofsted, Department for Education (DfE), Governor support services.
- Security organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

Department for Education (DfE)
The Department for Education (DfE) collects personal data from educational providers and local authorities. We are required to share information about individuals in governance roles with the Department for Education (DfE), under: section 538 of the Education Act 1996

All data is entered manually on the GIAS service and held by the Department for Education (DfE) under a combination of software and hardware controls which meet the current government security policy framework.
For more information, please see the 'How Government uses your data' section.
We may also share information with other third parties where there is a lawful basis to do so. For example, we sometimes share information with the police for the purposes of crime detection or prevention.

Storing governance information
We will retain your information in accordance with our retention schedule. The retention period for most of the information we process about you is determined by statutory obligations. Any personal information which we are not required by law to retain will only be kept for as long as is reasonably necessary to fulfil its purpose.

We may also retain some information for historical and archiving purposes in accordance with our retention schedule.

Requesting access to your personal data
The UK GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact [school business manager]

Your rights include

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request (SAR), data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'.
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances.
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why your information rights request may be refused. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at raise a concern with ICO

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the How Government uses your data section of this notice.

Withdrawal of consent and the right to lodge a complaint
Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the School Business Manager.

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact the School Business Manager.

If we cannot resolve your concerns then you may also complain to the Information Commissioner's Office, which is the UK's data protection regulator. Their contact details are below:
Phone: 0303 123 1113 Opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form.

Last Updated
We reserve the right to change this privacy notice at any time. We will normally notify you of changes that affect you. However, please check regularly to ensure you have the latest version.

This privacy notice was last reviewed 11 March 2026

Contact
If you would like to discuss anything in this privacy notice, please contact: School Business Manager email administration@rutlish.merton.sch.uk

Our Data Protection Officer is:schoolsDPO@merton.gov.uk

How government uses your data

The governance data that we lawfully share with the Department for Education (DfE) via GIAS will:

- increase the transparency of governance arrangements
- enable local authority-maintained schools, academies, academy trusts and the Department for Education (DfE) to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context
- allow the Department for Education (DfE) to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role

Data collection requirements
To find out more about the requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors

Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to authorised Department for Education (DfE) and education establishment users with a Department for Education (DfE) Sign-in account who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the Department for Education (DfE) unless the law allows it.

How to find out what personal information the Department for Education (DfE) hold about you
Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a subject access request (SAR). Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:
https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter
To contact DfE: https://www.gov.uk/contact-dfe

APPENDIX 7

Appropriate Policy Document

Contents

1. Introduction

1.1 Schedule 1, Part 4 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category data and criminal offence data under certain specified conditions. This is the 'Appropriate Policy Document' for Rutlish School.

1.2 The purpose of this statutory policy is to explain the basis on which we process special category and criminal convictions data and to demonstrate that our processing is compliant with principles set out in data protection legislation.

2. Special category data

2.1 Special category data is defined as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health, or
- Data concerning a natural person's sex life or sexual orientation.

3. Criminal convictions and offences data

3.1 Article 10 UK GDPR covers processing in relation to criminal convictions and offences. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes "*personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing"*. This is collectively referred to as 'criminal offence data'.

4. Conditions for processing special category and criminal offence data

4.1 Within the UK GDPR, all processing of special category data must meet an Article 9(2) condition in order for that processing to be lawful. The Article 9(2) conditions for processing special category data are:

Article 9(2)(a) Explicit consent
Article 9(2)(b) Employment, social security and social protection
Article 9(2)(c) Vital interests
Article 9(2)(d) Not-for-profit bodies
Article 9(2)(e) Made public by the data subject
Article 9(2)(f) Legal claims or judicial acts
Article 9(2)(g) Reasons of substantial public interest (with a basis in law)
Article 9(2)(h) Health or social care (with a basis in law)
Article 9(2)(i) Public health (with a basis in law)
Article 9(2)(j) Archiving, research and statistics (with a basis in law)

4.2 If processing is reliant on conditions (b), (h), (i) or (j), an associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018 must be met.

4.3 If processing is reliant on Article 9(2)(g) Reasons of substantial public interest, an associated condition in UK law, set out in Part 2 of Schedule 1 of the DPA 2018 must be met.

4.4 The school processes special category data under the following Article 9 and Schedule 1 conditions:

Article 9 condition	Examples of Processing	Schedule 1 Condition (where required)
Article 9(2)(a) data subject has given explicit consent	E.g. processing student and staff dietary requirements or consent for student pastoral support.	Not required
Article 9(2)(b) necessary in the field of employment law.	E.g. processing staff sickness absences, recording details of trade union membership, processing criminal offence data for the purposes of preemployment checks and declarations by an employee in line with contractual obligations.	**Part 1, Schedule 1 condition:** Para 1: Employment, social security and social protection
Article 9(2)(c) necessary to protect the vital interests of the data subject	E.g. using health information about a member of staff or a student in a medical emergency.	Not required
Article 9(2)(f) necessary for the establishment, exercise or defence of legal claims.	E.g. processing relating to any employment tribunal or other litigation.	Not required
Article 9(2)(g) necessary for reasons of substantial public interest.	E.g. processing student health information in order to ensure they receive appropriate educational support. Identifying individuals at risk by recording and reporting concerns from students and staff Obtaining further support for children and individuals at risk by sharing information with relevant agencies.	**Part 2, Schedule 1 conditions:** Para 6(1) and (2)(a): Statutory etc. and government purposes Para 8(1) and (2): Equality of opportunity or treatment Para 10(1): Preventing or detecting unlawful acts Para 16(1): Support for individuals with a particular disability or medical condition Para 18(1): Safeguarding of children and of individuals at risk
Article 9(2)(h)	E.g. the provision of occupational health services to our employees.	**Part 1, Schedule 1 condition:**
Article 9 condition	**Examples of Processing**	**Schedule 1 Condition (where required)**
necessary to assess the working capacity of the employee.		Para 1: Employment, social security and social protection

Article 9(2)(j) for archiving purposes in the public interest.	E.g. maintaining a school archive of photos and significant school events for historical purposes.	**Part 1, Schedule 1 condition:** Paragraph 4 Research etc

5. How we are compliant with the data protection principles

5.1 Principle (a): **Personal data shall be processed lawfully, fairly and in a transparent manner** in relation to the data subject. The school will ensure that:

- for each occasion where we process personal data, we have established the lawful basis of the processing under the UK GDPR
- where our processing is based on explicit consent, we have taken steps to ensure clear, freely given consent has been given and is recorded. We have made it clear to all parties how consent can easily be withdrawn at any time
- we provide clear and transparent information about why we process personal data through our privacy notices and associated policies
- a Data Protection Policy is established for the protection of personal data held within Rutlish School. This has been approved by governors and communicated to all employees and other relevant people.

5.2 Principle (b): **Personal data shall be collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. The school will ensure that:

- we only collect personal data for specified, explicit and legitimate purposes, and, having regard for the purpose of the processing, we will inform data subjects what those purposes are in a privacy notice
- we do not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, and having regard for the purpose of the processing, we will inform the data subject first.

5.3 Principle (c): **Personal data shall be adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation'). The School will ensure that:

- we collect personal data necessary for the relevant purposes and ensure it is not excessive
- the information we process is necessary for and proportionate to our purposes
- where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

5.4 Principle (d): **Personal data shall be accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'). The school will ensure that:

- where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed
- we will take every reasonable step to ensure that data is erased or rectified without delay
- if we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

5.5 Principle (e): **Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; ('storage limitation').

The school will ensure that:

- all special category data processed by us is retained for the periods set out in our Retention Schedule
- we determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

5.6 Principle (f): **Personal data shall be processed in a manner that ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss,

destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

The school will ensure that:

- data protection by design is at the heart of developing and maintaining our core systems and procedural developments
- all employees have completed mandatory training and receive annual refresher training in meeting their responsibilities under data protection legislation
- all of our employees are subject to confidentiality obligations with respect to personal data
- where we use data processors to process any personal data on our behalf, we have established data processing agreements
- routine data transfers that are necessary for our core school business processes are secure and use industry standard encryption methods. We regularly review our processes for data transfer in line with new technological developments.
- we have a robust IT infrastructure which has been implemented using the secure by design principle and we hold the Cyber Essentials Plus certification to guard against the most common cyber threats and demonstrate our commitment to cyber security
- hard copy information is processed in line with our security procedures
- our electronic systems and physical storage have appropriate access controls applied.

6. Review

6.1 The school will be responsible for ensuring that this policy is maintained and reviewed at regular intervals.

7. Other Documentation

This policy should be read in conjunction with:

- Data Protection Policy
- Records Management Policy
- Records Retention and Disposal Schedule
- Data Breach Guidance
- Privacy Notices