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 2023
Date of next review:	Spring 2026
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

1. 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

2. 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 which will adopt the UK GDPR, DPLED and The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data into UK law in the wake of the UK's exit from the European Union.
- 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

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'

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

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** 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.
he 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;

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.

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.

6. PRINCIPLES

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

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. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

13.1 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.

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.

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

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.

13.2 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.

14. 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.

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 pupil records to and from other schools in a machine-readable format.

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

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

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

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.
We will respond to any requests for portability within one month.

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

Individuals have the right to object to the following:
- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests
- An individual's grounds for objecting must relate to his or her particular situation.
- We will stop processing the individual's personal data unless the processing is for the establishment, exercise or 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 protection by design and privacy impact assessments
We will act in accordance with the UK GDPR by adopting a data protection by design approach and implementing technical and organisational measures which demonstrate how we has considered and integrated data protection into processing activities.

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

DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to this school's reputation which might otherwise occur.
A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

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

High risk processing includes, but is not limited to, the following:
- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- We will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

15. 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 pupils 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 pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
b) Storing pupils' 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 pupils.

16. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

a) Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
b) Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
c) Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

d) Integrating data protection into internal documents including this policy, any related policies and privacy notices
e) Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
f) Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
g) Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
h) Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

17. 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

18. 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.

Wi-Fi access to the school network is permitted from school devices. 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.

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 pupil sensitive information given to parents/visitors supporting the school visit should be on a 'need to know' basis only e.g. only the medical conditions of the children in their group should be shared.
- All documentation given to additional adults should be collected back at the end of the visit by the party leader.

19. **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.

20. **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.

21. 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.

22. 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.

23. 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.

24. **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.

25. **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 identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

Data controller – 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.

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

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

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

APPENDIX 2

RUTLISH SCHOOL

PRIVACY NOTICE – Parents/Carers

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 notice is to help you understand how and why we collect personal information about you and what we do with that information. It also explains the decisions that you can make about your own information. If you have any questions about this notice, please contact us (see 'Contact us' below).

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.

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).

What is "personal data"?

Personal data is data that the school holds about you and which identifies you. This includes data such as your date of birth and address as well as things like ethnicity and National Insurance details. CCTV, photos and video recordings of you are also personal data.

What is "personal information"?

Personal information is information that identifies you as an individual. This includes your contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information, but is not restricted to:

The categories of pupil 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)

The Personal data we hold

We set out below examples of the different ways in which we may collect, use, store and share (when appropriate) your personal information, but is not restricted to: The school's primary reason for using your personal information is to provide an education to your child:

- We obtain information about you from admissions forms and from your child's previous school. We may have information about any family circumstances which might affect your child's welfare or happiness.
- We may store bank details for school payments and refunds.
- We may need information about any court orders or criminal petitions which relate to you. This is so that we can safeguard the welfare and wellbeing of your child and the other students at the school.
- We may send you information to keep you up to date with what is happening at the school. For example, by sending you information about events and activities taking place (including fundraising events) and the School newsletter.
- We may use information about you if we need this for historical research purposes or for statistical purposes.
- Records of any correspondence and contact with us.
- Details of any complaints you have made.
- To comply with our legal and statutory obligations.

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:

- We may also get information from professionals such as doctors and from local authorities.
- We use CCTV to make sure the school site is safe.
- We may take photographs or videos of you at school events to use on social media and on the school website. This is to show prospective parents and 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.

We may also hold data about you that we have received from other organisations, including other schools and social services.

Why we use this data

We use the data listed above to:

a) Report to you on your child's attainment and progress
b) Keep you informed about the running of the school (such as emergency closures) and events
c) Process payments for school services and clubs
d) Provide appropriate pastoral care
e) Protect pupil welfare
f) Administer admissions waiting lists
g) Assess the quality of our services
h) Carry out research
i) Comply with our legal and statutory obligations

Use of your personal data for marketing purposes

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.

Our legal grounds for using your information

This section contains information about the legal basis that we are relying on when handling your child's information.

Public Interest

This means that the processing of your data is necessary for public interests. The school relies on public interests for most of the ways in which it uses your 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 students.
- 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 the school office.

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

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 the school office if you would like to withdraw any consent given.

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.

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 your rights or freedoms.

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.

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.

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 would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way.
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for the establishment, exercise or defence of legal claims.
- We need to process it for reasons of substantial public interest as defined in legislation.
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- We need to process it for reasons of substantial public interest as defined in legislation.

Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Your young people
- Police forces, courts, tribunals

Storing this data

We keep personal information about you while your young person is attending our school. We may also keep it beyond their attendance at our school if this is necessary. Our Data Protection Policy sets out how long we keep information about parents and carers.

To request a copy of your record retention schedule, please contact us (see 'Contact us' below).

We have put in place appropriate security measures to prevent your personal information being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.
We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- In accordance with our legal obligations, we may share information with The London Borough of Merton and other local authorities, the Department for Education and Ofsted for example, where we have any safeguarding concerns, leaves to attend another school.
- On occasion, we may need to share information with the police in cases of emergency.
- We may also need to share information with our legal advisers for the purpose of obtaining legal advice.
- 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 information with them if this is relevant to their work.
- We may share some information with our insurance company, for example, where there is a serious incident at the School.
- We may share information about you with others in your family, such as another parent or step-parent. For example, where this is part of our obligation to take care of your child, as part of our wider legal and regulatory obligations.
- We may need to share with Health Authorities information if there is an emergency, for example, if you are hurt whilst on School premises.
- Charities and voluntary organisations for example the school's PTA
- Suppliers and service providers for example exam centres, catering companies, trip and residential companies this is not limited to.

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.

Your Rights
How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data
Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data.
- Prevent your data being used to send direct marketing.
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person).
- In certain circumstances, have inaccurate personal data corrected.
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing.
- In certain circumstances, be notified of a data breach.
- Make a complaint to the Information Commissioner's Office.
- Claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints
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.

Alternatively, you can make a complaint to the Information Commissioner's Office:

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

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

Our data protection officer is: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 email administration@rutlish.merton.sch.uk

Changes to this notice
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.

RUTLISH SCHOOL

PRIVACY NOTICE – Students

HOW WE USE YOUR INFORMATION

Introduction
This notice is to help you understand how and why we collect your personal information and what we do with that information. It also explains the decisions that you can make about your own information.

We are giving you this notice because you are mature enough to make decisions about your personal information.

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).

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

What is "personal data"?
Personal data is data that the school holds about you and which identifies you. This includes data such as your date of birth and address as well as things like ethnicity and National Insurance details. CCTV, photos and video recordings of you are also personal data.

What is "personal information"?
Personal information is information that the school holds about you and which identifies you. This includes information such as your name, date of birth and address as well as things like exam results, medical details and behaviour records. The school may also record your religion or ethnic group. CCTV, biometric data, photos and video recordings of you are also personal information.

Personal information that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your contact details
- Your test/exams results
- Your attendance records
- Details of any behaviour issues or exclusions
- Online identifier, such as a username

The personal data we hold
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 your characteristics, like your ethnic background or any special educational needs, nationality and religion
- Information about any medical conditions you have
- Photographs and CCTV images
- Biometrics (fingerprints), used for identification purpose
- Medical
- Health – Physical or mental
- Educational needs

Why we use this data
We use the data listed above to:

a) Get in touch with you and your parents when we need to
b) Support student learning
c) monitor your progress in lessons and exams, and work out whether you need additional support

d) Track how well the school as a whole is performing
e) Look after your wellbeing
f) To pay for school meals
g) To monitor your use of email, internet and mobile devices
h) Admissions waiting lists (RR6)
i) Carry out research

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

You can take back this 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 put your personal information through any automated decision making or profiling process. This means we do not make decisions about you using only computers without any human involvement.

If this changes in the future, we will update this notice in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this information
We will only collect and use your information when the law allows us to. We need to establish a 'lawful basis' to do this.

Our lawful bases for processing your personal information for the reasons listed in section 3 above are:

Public interests
This means that the processing of your data is necessary for public interests. The School relies on public interests for most of the ways in which it uses your data.

Specifically, the school has a public interest in:

- Providing you with an education.
- Safeguarding and promoting your welfare and the welfare of other young people.
- 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.

Legal obligation
Where the School needs to use your information in order to comply with a legal obligation, for example under the Education Act, Keeping Young people Safe in Education should the school need to report a concern about your wellbeing to Young people's Services.

Consent
The school may request your consent and must be freely given and actively opt in for the use of photographs, videos and biometrics.

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.

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 your rights or freedoms.

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.

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.

Where you have provided us with consent to use your information, you may take back this consent at any time. We will make this clear when requesting your consent, and explain how you'd go about withdrawing consent if you want to.

Our basis for using special category data
For 'special category' data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your information in a certain way.
- We need to use your information under employment, social security or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The information has already been made obviously public by you.
- We need to use it to make or defend against legal claims.
- We need to use it for reasons of substantial public interest as defined in legislation.
- We need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law.
- We need to use it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law.
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made obviously public by you.
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims.
- We need to use it for reasons of substantial public interest as defined in legislation.

Collecting this data
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with Data Protection law, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Whenever we want to collect information from you, we make it clear if you have to give us this information (and if so, what the possible consequences are of not doing that), or if you have a choice.

Some of the data we hold about you will come from you, but we may also hold data about you from:

- Your parents/carers
- Local councils
- Government departments or agencies
- Police forces, courts, tribunals

Storing this data
We keep personal information about you while you're attending our school. We may also keep it beyond your attendance at our school if this is necessary. Our record retention schedule sets out how long we keep information about students.

To request a copy of your record retention schedule, please contact us (see 'Contact us' below).
We have security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share data with
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.

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 London Borough of Merton – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions.
- Government departments or agencies – to meet our legal obligations to collect data e.g. census.
- Other schools if students leave.
- 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 service.

National Pupil Database
We have to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations, such as organisations that promote young people's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

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 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 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.

Your rights

How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (unless there's a really good reason why we shouldn't):

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data (decisions made by a computer or machine, rather than by a person), and any consequences of this
- Give you a copy of the information in an understandable form

You may also have the right for your personal information to be shared with another organisation in certain circumstances. If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data

Under UK data protection law, you have certain rights regarding how your personal information is used and kept safe. For example, you have the right to:

- Say that you do not want your personal information to be used
- Stop it being used to send you marketing materials
- Say that you do not want it to be used for automated decisions (decisions made by a computer or machine, rather than by a person)
- In some cases, have it corrected if it's inaccurate
- In some cases, have it deleted or destroyed, or restrict its use
- In some cases, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints

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.

Alternatively, you can make a complaint to the Information Commissioner's Office:

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

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Our Data Protection Officer is: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 email administration@rutlish.merton.sch.uk

Changes to this notice

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.

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. If you have any questions about this notice, please talk to the School Business Manager (see 'Contact us' below).

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).

What is "personal information"?
Personal information is information that the school holds about you and which identifies you. This includes information such as your date of birth and address as well as things like ethnicity and National Insurance details. CCTV, photos and video recordings of you are also personal information.

The personal data we hold
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

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:

- Any health conditions you have that we need to be aware of
- Sickness records
- Photographs and CCTV images captured in school
- Trade union membership

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 use this data
We use the data listed above to:

- Enable you 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

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.

Our legal grounds for using your information
This section contains information about the legal basis that we are relying on when handling your information.

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

- Providing young people with an education.
- Safeguarding and promoting the welfare of young people.
- 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.
-

In addition, your personal information may be processed for the public interests of others. For example, we may use information when investigating a complaint.

Legal obligation
Where the school needs to use your information in order to comply with a legal obligation, for example to report a concern about a young person's wellbeing to Young People's Services, we may also have to disclose your information to third parties such as the courts, the Local Authority or the police where legally obliged to do so.

Consent
The school may request your consent and must be freely given and actively opt in. for the use of photographs, biometrics.

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.

Contract basis
To process personal data to fulfil a contract with you or to help you enter into a contract with us

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 your rights or freedoms.

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.

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 would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way.
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for the establishment, exercise or defence of legal claims.
- We need to process it for reasons of substantial public interest as defined in legislation.
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- We need to process it for reasons of substantial public interest as defined in legislation.

Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals
- Previous employer or education setting

How we store this data

We keep personal information about you while you are attending our school. We may also keep it beyond your attendance at our school if this is necessary. Our record retention schedule sets out how long we keep information about students.

To request a copy of your record retention schedule, please contact us (see 'Contact us' below).

We have security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

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

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 London Borough of Merton – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Government departments or agencies to meet our legal obligations to collect data
- Our regulator, Ofsted
- Suppliers and service providers: catering services trips and residential companies and other schools
- Financial organisations to be able to pay online
- Our auditors
- Survey and research organisations
- Health authorities e.g. if you had an accident at work
- Security organisations e.g. biometric system use by the catering company
- Health and social welfare organisations external HR services
- Professional advisers and consultants external HR services
- Police forces, courts, tribunals the school may be required to share information to these services, DBS

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.

Your rights
How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you. If you make a subject access request, and if we do hold information about you, we will (unless there's a really good reason why we shouldn't):

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data (decisions made by a computer or machine, rather than by a person), and any consequences of this
- Give you a copy of the information in an understandable form

You may also have the right for your personal information to be shared with another organisation in certain circumstances. If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data
Under data protection law, you have certain rights regarding how your personal information is used and kept safe. For example, you have the right to:

- Say that you do not want your personal information to be used
- Stop it being used to send you marketing materials
- Say that you do not want it to be used for automated decisions (decisions made by a computer or machine, rather than by a person)
- In some cases, have it corrected if it's inaccurate
- In some cases, have it deleted or destroyed, or restrict its use

- In some cases, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints
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.

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

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Our Data Protection Officer is: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 email administration@rutlish.merton.sch.uk

Changes to this notice
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.

APPENDIX 5

RUTLISH SCHOOL

PRIVACY NOTICE – Recruitment

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 applying for jobs at our school. If you have any questions about this notice, please talk to the School Business Manager (see 'Contact us' below).

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).

What is "personal data"?

Personal data is data that the school holds about you and which identifies you. This includes data such as your date of birth and address as well as things like ethnicity and National Insurance details. CCTV, photos and video recordings of you are also personal data.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- personal data such as name, date of birth, contact details, National Insurance number, teacher number (if applicable).
- Copies of right to work documentation
- References
- Evidence of qualifications and proof of your identity, if invited for interview.
- Employment records, including work history, job titles, training records and professional memberships
- Data about any reasonable adjustments we need to make to the shortlisting or interview and assessment process to accommodate a disability.
- Data about any cautions, convictions, reprimands or final warnings which are not protected, as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended) as well as any current police investigations or pending criminal proceedings.

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
- Information about disability and access requirements
- Photographs and CCTV images captured in school

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 use this data

We use the data listed above to:

- Enable us to establish relevant experience and qualifications
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Enable equalities monitoring
- Ensure that appropriate access arrangements can be provided for candidates that require them

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.

The lawful basis on which we process this data
Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:
Public Interest

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

- Providing young people with an education.
- Safeguarding and promoting the welfare of young people.
- 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.

In addition, your personal information may be processed for the public interests of others. For example, we may use information when investigating a complaint.

Legal obligation
We process special category data, such as data about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations (such as the requirement to make reasonable adjustments for job applicants with a disability) and in particular with the Department for Education statutory guidance document, Keeping Young People Safe in Education, such as by carrying out pre-employment checks on your right to work in the UK and with the Disclosure and Barring Service.. This data is collected with the express consent of job applicants. Consent may be withdrawn by an applicant at any time.

Consent
Personal data provided to us as part of the recruitment and selection process is generally given on a voluntary basis and, as such, you have a choice as to whether you provide data to us. However, failure to provide data may mean that your application cannot be processed. You should also be aware that providing false or misleading data (including by omission) may result in your application being rejected and could also be treated as a disciplinary offence in the event that employment is subsequently offered to you.

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.

Contract basis
To process personal data to fulfil a contract with you or to help you enter into a contract with us

Legitimate interest
We have a legitimate interest in processing data from job applicants in order to administer the recruitment process, to monitor compliance with our policies, to defend any legal claims and to ensure that the most suitable applicant is appointed to the role, based on an assessment of their likely performance amongst other factors. We do not rely on legitimate interests as a reason for processing data unless we have first considered the rights and freedoms of the individuals affected and determined that these do not override the interests we have identified.

We may offer to contact unsuccessful applicants within a period of six months following the application if another suitable vacancy arises. Information is only used in this way with the express consent of applicants, which may be withdrawn at any time.

If we wish to process your personal data for a new purpose we will inform you of any additional processing.

Posts in our organisation are exempt from the Rehabilitation of Offenders Act 1974 (as amended). If you decide to submit an application form, you must disclose any cautions and convictions, even if they are spent, other than protected cautions and convictions (i.e. those which have been filtered out). Details on the filtering rules applicable to certain offences can be found on the Gov.uk website: https://www.gov.uk/government/collections/dbs-filtering-guidance .

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way.
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for the establishment, exercise or defence of legal claims.
- We need to process it for reasons of substantial public interest as defined in legislation.
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- We have obtained your consent to use it in a specific way.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent.
- The data concerned has already been made manifestly public by you.
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- We need to process it for reasons of substantial public interest as defined in legislation.

Collecting this data
While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.
Adapt the list below to reflect the sources of any data you've obtained from anyone other than the applicant.
Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals

Storing this data
We keep personal information about you during the application process. We may also keep it beyond this if this is necessary. Our retention schedule document sets out how long we keep information about applicants.

Explain how to request a copy of your record retention schedule document.

Information from your application form and from the shortlisting and selection process will be stored in a paper-based file, in electronic records within our HR system and also in other IT systems, including email.

A copy of your application form and all other personal data collected during the recruitment and selection process will be held as follows:

- For successful applicants this will be transferred to a personnel file where it will be held securely. You will be given a workforce privacy notice upon appointment which will explain how we will hold and process your data as an employee.
- For unsuccessful applicants, securely for a period of six months.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.
We will dispose of your personal data securely when we no longer need it.

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

Where it is legally required, or necessary (and it complies with UK data protection law), we may share personal information about you with:

- Our local authority London Borough of Merton – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as HR and recruitment support
- Professional advisers and consultants
- Employment and recruitment agencies

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.

Your rights
How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Prevent your data being used to send direct marketing

- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints

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.

Alternatively, you can make a complaint to the Information Commissioner's Office:

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

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Our Data Protection Officer is: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 email administration@rutlish.merton.sch.uk.

Changes to this notice

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.

APPENDIX 6

RUTLISH SCHOOL

PRIVACY NOTICE – Governors and other volunteers

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 working with our school in a voluntary capacity, including governors. If you have any questions about this notice, please talk to the School Business Manager (see 'Contact us' below).

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).

What is "personal data"?
Personal data is data that the school holds about you and which identifies you. This includes data such as your date of birth and address as well as things like ethnicity and National Insurance details. CCTV, photos and video recordings of you are also personal data.

The personal data we hold
Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- References
- Evidence of qualifications and proof of your identity
- Employment details
- Information about business and pecuniary interests

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 any health conditions you have that we need to be aware of
- Information about disability and access requirements
- Photographs and CCTV images captured in school

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 use this data
We use the data listed above to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing governors' details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring
- Ensure that appropriate access arrangements can be provided for volunteers who require them

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.

The lawful basis on which we process this data
Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

Public Interest
This means that the processing of your data is necessary for public interests. The school relies on public interests for most of the ways in which it uses your data:

- Providing young people with an education.
- Safeguarding and promoting the welfare of young people.
- 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.

In addition, your personal information may be processed for the public interests of others. For example, we may use information when investigating a complaint.

Legal obligation
We process special category data, such as data about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations (such as the requirement to make reasonable adjustments for job applicants with a disability) and in particular with the Department for Education statutory guidance document, Keeping Young People Safe in Education, such as by carrying Disclosure and Barring Service. 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.

Consent
The school may obtain consent from you to use your personal data and must be freely given and actively opt in. If you change your mind you have the right to withdraw that consent, please let us know.

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.

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 your rights or freedoms.

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 would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the applicant.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals

Storing this data

We keep personal information about you during the application process. We may also keep it beyond this if this is necessary. Our retention schedule document sets out how long we keep information about applicants.

Explain how to request a copy of your record retention schedule document.

Information from your application form and from the shortlisting and selection process will be stored in a paper-based file, in electronic records within our HR system and also in other IT systems, including email.

A copy of your application form and all other personal data collected during the recruitment and selection process will be held as follows:

- For successful applicants this will be transferred to a personnel file where it will be held securely. You will be given a workforce privacy notice upon appointment which will explain how we will hold and process your data as an employee.
- For unsuccessful applicants, securely for a period of six months.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share this data with

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

Where it is legally required, or necessary (and it complies with UK data protection law), we may share personal information about you with:

- Our local authority London Borough of Merton – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Governments departments or agencies
- Our regulator, Ofsted, Department for Education (DfE), Governor support services
- Disclosure and Barring Service (DBS).
- Our auditors
- Health authorities
- Security organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

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.

Your rights

How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data

Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints

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.

Alternatively, you can make a complaint to the Information Commissioner's Office:

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

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Our Data Protection Officer is: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 email administration@rutlish.merton.sch.uk.

Changes to this notice
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.

APPENDIX 7

RUTLISH SCHOOL

PRIVACY NOTICE – General

Introduction

Under UK data protection law, this privacy notice has been written to inform individuals who come into contact with or visit Rutlish School about how and why we process your personal data. It includes when we process information relating to general queries and complaints. 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 supplements the school's other notices for pupils and parents, the workforce, and governors and volunteers.

If you have any questions about this notice, please talk to the School Business Manager (see 'Contact us' below).

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).

Who are we?

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 LB 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 is "personal data"?

Personal data is data that the school holds about you and which identifies you. This includes data such as your date of birth and address as well as things like ethnicity and National Insurance details. CCTV, photos and video recordings of you are also personal data.

What personal information do we collect?

The personal data we collect about you will be dependent on the nature of your contact and relationship with us, but could include:

- Contact details
- Personal details, including name, address and contact information.
- Company details and contact information, if appropriate.
- Details of the reasons for contact with the school, and any communication preferences.
- Visitor information, such as the purpose of your visit and time you enter and leave the school, car registration number and any health conditions or disability access needs you tell us about.
- Records of communications and interactions we have with you.
- Any details provided by yourself or third parties relating to a complaint investigation, including witness statements and interview notes.
- Information required for the school admissions process. This includes:
    - Identifiers and contact details
    - Reasons for the application
    - SEN and/or Looked After status and history
    - Relevant safeguarding information and professional involvement - Equality information, such as ethnicity and gender.
    - Characteristics including free school meal eligibility and language spoken
    - Name of current and any previous school(s)
    - Previous educational and assessment attainments

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 disability and access requirements
- Photographs and CCTV images captured in school

Why do we collect your personal information?

We process your information for the purposes outlined below:

- To effectively respond to your query or request.
- To comply with a legal or regulatory obligation such as safeguarding and health and safety requirements.
- To process feedback and improve our services.
- To promote the school, including in newsletters, on the school website and social media platforms.
- To effectively administer the school's complaints process.
- To monitor and inform our policies on equality and diversity.
- Protect pupil welfare
- Comply with our legal and statutory obligations

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.

The lawful basis on which we process this data

Under the UK GDPR, it is essential to have a lawful basis when processing personal information. We normally rely on the following lawful bases:

Public Interest

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

- Providing young people with an education.
- Safeguarding and promoting the welfare of young people.
- 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.

In addition, your personal information may be processed for the public interests of others. For example, we may use information when investigating a complaint.

Legal obligation

We process special category data, such as data about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations (such as the requirement to make reasonable adjustments for job applicants with a disability) and in particular with the Department for Education statutory guidance document, Keeping Young People Safe in Education and with the Disclosure and Barring Service.

Consent

The school may obtain consent from you to use your personal data and must be freely given and actively opt in. If you change your mind you have the right to withdraw that consent, please let us know.

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.

Legitimate interest
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.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way.
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law.
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you are physically or legally incapable of giving consent.
- We need to process it for the establishment, exercise or defence of legal claims.
- We need to process it for reasons of substantial public interest as defined in legislation.
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

Collecting this data
While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.
Adapt the list below to reflect the sources of any data you've obtained from anyone other than the applicant.
Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts, tribunals

Storing this data
We will retain your information in accordance with our retention schedule document. 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 document.

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

- Department for Education (DfE).
- Local Authority.
- Ofsted.
- Information Commissioner's Office and/or Local Government Ombudsman.

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.

Transferring data internationally
Although we are based in the UK, some of the digital information we hold may be stored on computer servers located outside the UK. Some of the IT applications we use may also transfer data outside the UK.
Normally your information will not be transferred outside the European Economic Area, which is deemed to have adequate data protection standards by the UK government. In the event that your information is transferred outside the EEA, we will take reasonable steps to ensure your data is protected and appropriate safeguards are in place.

Your rights

How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.
If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact us (see 'Contact us' below).

Your other rights regarding your data

Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' below).

Complaints

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.

Alternatively, you can make a complaint to the Information Commissioner's Office:

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

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Our Data Protection Officer is: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 email administration@rutlish.merton.sch.uk.

Changes to this notice

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.

APPENDIX 8

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 pupil and staff dietary requirements or consent for pupil 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 pupils 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