RICKMANSWORTH SCHOOL

Data Protection Policy 2023-2024

Version:	5
Version Author:	Emma Gritten
Version Ratified By:	Board of Trustees
Date Version Ratified:	September 2023
Trustee's Lead:	David Wellings
SLT's Lead	Emma Gritten
Date this version issued:	September 2023
Last Review Date:	September 2022
Next Review Date:	September 2024
Target Audience:	Trustees, Staff, Parents
To Be Published on The Website	Yes

Table of Contents

OVERVIEW

Purpose

The objectives of this Data Protection Policy are to ensure that Rickmansworth School (the "School") and its governors and employees are informed about, and comply with, their obligations under the UK General Data Protection Regulation ('**UK GDPR**'), the Data Protection Act 2018 ('**DPA**'), and other regulations (together 'the **UK Data Protection Legislation**').

A reference copy of this document is kept on the shared drive and it will be brought to the attention of all members of staff.

Review Process

This document will be reviewed in accordance with our policy review process on a yearly basis or on the introduction of new or amended relevant legislation.

Tony Walker
CHAIR OF GOVERNORS

Matt Fletcher
HEADTEACHER

1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that Rickmansworth School (the "School") and its governors and employees are informed about, and comply with, their obligations under the UK General Data Protection Regulation ("the UK GDPR") and other data protection legislation.

1.2 The School is an Academy school and is the Data Controller for all the Personal Data processed by the School.

1.3 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

1.4 The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, students, parents / carers and other members of students' families, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK GDPR and other legislation. The UK GDPR imposes restrictions on how we may use that information.

1.5 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the UK GDPR may expose the School to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the School's employees. At the very least, a breach of the UK GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

2. Status of the policy

2.1 This policy has been approved by the Governing Body of the School. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3. Data Protection Officer

3.1 The Data Protection Officer (the "DPO") is responsible for ensuring the School is compliant with the UK data protection legislation and with this policy. This post is held by Mr Matthew Lantos, DPO@rickmansworth.herts.sch.uk. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

3.2 The DPO will play a major role in embedding essential aspects of the UK GDPR into the School's culture, from ensuring the data protection principles are

respected to preserving data subject rights, recording data processing activities and ensuring the security of processing.

3.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the UK GDPR requires that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

- 3.3.1 senior management support;
- 3.3.2 time for DPOs to fulfil their duties;
- 3.3.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;
- 3.3.4 official communication of the designation of the DPO to make known existence and function within the organisation;
- 3.3.5 access to other services, such as HR, IT and security, who should provide support to the DPO;
- 3.3.6 continuous training so that DPOs can stay up to date with regard to data protection developments;
- 3.3.7 where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;
- 3.3.8 whether the School should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

3.4 The DPO is responsible for ensuring that the School's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the School must ensure the independence of the DPO.

3.5 The School will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the Governing Body.

3.6 The requirement that the DPO reports directly to the Governing Body ensures that the School's governors are made aware of the pertinent data protection issues. In the event that the School decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

3.7 A DPO appointed internally by the School is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with his or her role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.

3.8 In order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing personal data. Senior management positions such as chief executive, chief financial officer, head of marketing, head of IT or head of human resources positions are likely to cause conflicts. Some other positions may involve

determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

3.9 In the light of this and in the event that the School decides to appoint an internal DPO, the School will take the following action in order to avoid conflicts of interests:

3.9.1 identify the positions incompatible with the function of DPO;

3.9.2 draw up internal rules to this effect in order to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate;

3.9.3 include a more general explanation of conflicts of interests; and

3.9.4 include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.

3.10 If you consider that the policy has not been followed in respect of Personal Data about yourself or others, you should raise the matter with the DPO.

4. Definition of terms

4.1 Biometric Data means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

4.2 Consent of the Data Subject 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 relating to him or her;

4.3 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

4.4 Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

4.5 Data Controllers means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

4.6 Data Users include employees, volunteers, governors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;

4.7 Data Processors means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

4.8 Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

4.9 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;

4.10 Personal Data Breach means 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;

4.11 Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR;

4.12 Processing means 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;

4.13 Special Category Data means 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.

5. Data protection principles

5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

5.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2 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;

5.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4 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;

5.1.5 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; and

5.1.6 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.

5.2 Processed lawfully, fairly and in a transparent manner

5.2.1 The UK GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the School), who the Data Controller's representative is (in this case the DPO), the purpose for which the data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

5.2.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

5.2.2.1 where we have the Consent of the Data Subject;

5.2.2.2 where it is necessary for compliance with a legal obligation;

5.2.2.3 where processing is necessary to protect the vital interests of the Data Subject or another person;

5.2.2.4 where it 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.

5.2.3 Personal data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

5.3 Special Category Data

5.3.1 The School will be processing Special Category Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Special Category Data.

5.3.2 When Special Category Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 5.1 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

5.3.2.1 the Data Subject's explicit consent to the processing of such data has been obtained

5.3.2.2 processing is necessary for reasons of substantial public interest, on the basis of UK law which shall be proportionate to the aim pursued, where we 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;

5.3.2.3 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;

5.3.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by UK law or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

5.3.3 The School recognises that in addition to Special Category Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Special Category Data.

5.4 Biometric Data

5.4.1 The School processes Biometric Data as part of an automated biometric recognition system, for cashless catering to provide him or her with services. Biometric Data is a type of Special Category Data.

5.4.2 Where Biometric Data relating to students is processed, the School must ensure that each parent of a child is notified of the school's intention to use the child's Biometric Data and obtain the written consent of at least one parent before the data is taken from the student and used as part of an automated biometric recognition system. The School must not process the Biometric Data if a student under 18 years of age where:

5.4.2.1 the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;

5.4.2.2 no Parent has consented in writing to the processing; or

5.4.2.3 a Parent has objected in writing to such processing, even if another Parent has given written Consent.

5.4.3 The School must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system. The School will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.

5.4.4 The School must obtain the explicit Consent of staff, governors, or other Data Subjects before Processing their Biometric Data

5.5 Criminal convictions and offences

5.5.1 There are separate safeguards in the UK GDPR for Personal Data relating to criminal convictions and offences.

5.5.2 It is likely that the School will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

5.5.3 In addition, from time to time we may acquire information about criminal convictions or offences involving students or Parents. This information is

not routinely collected and is only likely to be processed by the School in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

5.5.4 Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

5.6 Transparency

5.6.1 One of the key requirements of the UK GDPR relates to transparency. This means that the School must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

5.6.2 One of the ways we provide this information to individuals is through a privacy notice which sets out important information about what we do with their Personal Data. The School has developed privacy notices for the following categories of people:

5.6.2.1 Students, (Appendix 2)

5.6.2.2 Parents (Appendix 2)

5.6.2.3 Staff (Appendix 2)

5.6.2.4 Governors

5.6.3 The School wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to School premises or if we ask people to complete forms requiring them to provide their Personal Data.

5.6.4 We will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

5.7 Consent

5.7.1 The School must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

5.7.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.7.3 In the event that we are relying on Consent as a basis for Processing Personal Data about students, if a student is aged under 13, we will need to obtain Consent from the Parent(s). In the event that we require Consent for Processing Personal Data about students aged 13 or over, we will require the Consent of the student although, depending on the circumstances, the School should consider whether it is appropriate to inform Parents about this process. Consent is likely to be required if, for example, the School wishes to use a photo of a student on its website or on social media. Consent is also required before any students are signed up to online learning platforms. Such Consent must be from the Parent if the student is aged under 13. When relying on Consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

5.7.4 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.7.5 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Data. Often we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data.

5.7.6 Evidence and records of Consent must be maintained so that the School can demonstrate compliance with Consent requirements.

6. Specified, explicit and legitimate purposes

6.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any data which is not necessary for that purpose should not be collected in the first place.

6.2 The School will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

7. Adequate, relevant and limited to what is necessary

7.1 The School will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

7.2 In order to ensure compliance with this principle, the School will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

7.3 Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a school and we should not

collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

7.4 The School will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that the only members of staff or governors who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the School may adopt a layered approach in some circumstances, for example, members of staff or governors may be given access to basic information about a student or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Special Category Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

7.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the School's data retention guidelines.

8. Accurate and, where necessary, kept up to date

8.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

8.2 If a Data Subject informs the School of a change of circumstances their records will be updated as soon as is practicable.

8.3 Where a Data Subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

8.4 Notwithstanding paragraph 8.3, a Data Subject continues to have rights under the UK GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 8.3 has been followed.

9. Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed

9.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

9.2 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The School has a retention schedule for all data.

10. Data to be processed in a manner that ensures appropriate security of the Personal Data

10.1 The School has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

10.2 The UK GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

10.3 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

10.4 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

10.5 Data Users must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our Data Protection Policy and e-Safety Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

10.6 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

10.6.1 Confidentiality means that only people who are authorised to use the data can access it.

10.6.2 Integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed.

10.6.3 Availability means that authorised users should be able to access the data if they need it for authorised purposes.

10.7 It is the responsibility of all members of staff and governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher or the DPO.

10.8 Please see our Data Security Policy for details for the arrangements in place to keep Personal Data secure:

10.9 Governors

10.9.1 Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, student exclusions or parent complaints. Governors should be trained on the School's data protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

10.9.1.1 Ensure that Personal Data which comes into their possession as a result of their School duties is kept secure from third parties, including family members and friends;

10.9.1.2 Ensure they are provided with a copy of the School's Data Security Policy.

10.9.1.3 Using a School email account for any School-related communications;

10.9.1.4 Ensuring that any School-related communications or information stored or saved on an electronic device or computer is password protected and where required encrypted;

10.9.1.5 Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be accessed by third parties.

10.9.2 Governors will be asked to read and sign an Acceptable Use Agreement.

11. Processing in line with Data Subjects' rights

11.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

11.1.1 withdraw Consent to Processing at any time;

11.1.2 receive certain information about the Data Controller's Processing activities;

11.1.3 request access to their Personal Data that we hold;

11.1.4 prevent our use of their Personal Data for direct marketing purposes;

11.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

11.1.6 restrict Processing in specific circumstances;

11.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

11.1.8 request a copy of an agreement under which Personal Data is transferred outside of the UK;

11.1.9 object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);

11.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

11.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

11.1.12 make a complaint to the supervisory authority (the ICO); and

11.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

11.2 We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

12. Dealing with subject access requests

12.1 The UK GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The School can invite a Data Subject to complete a form but we may not insist that they do so.

12.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the UK GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the School from responding to the request as being made under the UK GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the UK GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

12.3 Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is one calendar month.

12.4 As the time for responding to a request does not stop during the periods when the School is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing the following measures:

12.5 Utilising a general Data Protection email address that will be monitored and if required has an out of office auto reply with appropriate statements.

12.6 A fee may not be charged to the individual for provision of this information.

12.7 The School may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

12.8 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

12.9 Requests from students who are considered mature enough to understand their rights under the UK GDPR will be processed as a subject access request as outlined below and the data will be given directly to the student (subject to any exemptions that apply under the UK GDPR or other legislation). As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when students may be considered mature enough to exercise their own subject access rights. In every case it will be for the School, as Data Controller, to assess whether the child is capable of understanding their rights under the UK GDPR and the implications of their

actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

12.10 Requests from students who do not appear to understand the nature of the request will be referred to their Parents or carers.

12.11 Requests from Parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the student is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the School considers the child to be mature enough to understand their rights under the UK GDPR, the School shall ask the student for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the School to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the School shall not disclose the Personal Data if to do so would breach any of the data protection principles.

12.12 It should be noted that the Education (Student Information) (England) Regulations 2005 (the "Regulations") applies to maintained schools only so the rights available to parents in those Regulations to access their child's educational records do not apply to the School. Therefore, if a parent of a student at an academy is applying for educational information, they must do so under the Data Protection Act 2018 (DPA 2018), which applies to personal data held anywhere, including by all types of school. Under the DPA 2018 the applicant parents will be exercising their child's right as the data subject to see his or her own educational records, on the child's behalf.

12.13 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made in the School's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

12.14 Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the School can:

12.14.1 charge a reasonable fee taking into account the administrative costs of providing the information; or

12.14.2 refuse to respond.

12.15 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.

12.16 Certain information may be exempt from disclosure, so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

12.17 In the context of a School a subject access request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

13. Providing information over the telephone

13.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the School whilst also applying common sense to the particular circumstances. In particular, they should:

13.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

13.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

13.1.3 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

14. Authorised disclosures

14.1 The School will only disclose data about individuals if one of the lawful bases apply.

14.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The School will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

14.2.1 Local Authorities
14.2.2 the Department for Education
14.2.3 the Disclosure and Barring Service
14.2.4 the Teaching Regulation Agency
14.2.5 the Teachers' Pension Service
14.2.6 the Local Government Pension Scheme which is administered by Local Government Pension Scheme
14.2.7 our external payroll provider Data Plan
14.2.8 our external IT Provider
14.2.9 HMRC
14.2.10 the Police or other law enforcement agencies
14.2.11 our legal advisors and other consultants
14.2.12 insurance providers
14.2.13 occupational health advisors
14.2.14 exam boards including AQA, Pearson, WJEC CBAC, OCR

14.2.15 the Joint Council for Qualifications;
14.2.16 NHS health professionals including educational psychologists and school nurses;
14.2.17 Education Welfare Officers;
14.2.18 Courts, if ordered to do so;
14.2.19 prevent teams in accordance with the Prevent Duty on schools;
14.2.20 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;
14.2.21 confidential waste collection companies;
14.2.22 some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches

14.3 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

14.4 All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

14.5 The UK GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is Processed ("GDPR clauses"). A summary of the UK GDPR requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the School to ensure that the UK GDPR clauses have been added to the contract with the Data Processor. Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

14.6 In some cases, Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the UK GDPR, including responsibility for any Personal Data Breaches, onto the School. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

15. Reporting a Personal Data Breach

15.1 The UK GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject, unless the data breach is unlikely to result in a risk to the individuals.

15.2 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours.

15.3 If the breach is likely to result in high risk to affected Data Subjects, the UK GDPR, requires organisations to inform them without undue delay.

15.4 It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

15.5 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

15.6 As the School is closed or has limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects when we develop our SECURITY INCIDENT RESPONSE PLAN.

15.7 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, our SECURITY INCIDENT RESPONSE PLAN must be followed. In particular, the DPO or such other person identified in our Security Incident Response Plan must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

16. Accountability

16.1 The School must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The School is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The School must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

16.2.1 appointing a suitably qualified DPO (where necessary) and an executive team accountable for data privacy;

16.2.2 implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;

16.2.3 integrating data protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;

16.2.4 regularly training employees and governors on the UK GDPR, this Data Protection Policy, related policies and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The School must maintain a record of training attendance by School personnel; and

16.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record keeping

17.1 The UK GDPR requires us to keep full and accurate records of all our Data Processing activities.

17.2 We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

17.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures

in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. Training and audit

18.1 We are required to ensure all School personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

18.2 Members of staff must attend all mandatory data privacy related training.

19. Privacy by Design and Data Protection Impact Assessment (DPIA)

19.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2 This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

19.2.1 the state of the art;

19.2.2 the cost of implementation;

19.2.3 the nature, scope, context and purposes of Processing; and

19.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

19.3 We are also required to conduct DPIAs in respect to high risk processing.

19.3.1 The School should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the processing of personal data including:

19.3.1.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

19.3.1.2 automated processing including profiling and ADM;

19.3.1.3 large scale processing of sensitive data; and

19.3.1.4 large scale, systematic monitoring of a publicly accessible area.

19.4 We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to students. If our processing is likely to result in a high risk to the rights and freedom of children, then a DPIA should be undertaken.

19.5 A DPIA must include:

19.5.1 a description of the Processing, its purposes and the School's legitimate interests if appropriate;

19.5.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

19.5.3 an assessment of the risk to individuals; and

19.5.4 the risk mitigation measures in place and demonstration of compliance.

20. CCTV

21. The School uses CCTV in locations around the School site. This is to:

21.1.1 protect the School buildings and their assets;

21.1.2 increase personal safety and reduce the fear of crime;

21.1.3 support the Police in a bid to deter and detect crime;

21.1.4 assist in identifying, apprehending and prosecuting offenders;

21.1.5 provide evidence for the School to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, students or other visitors on the site which breaches or is alleged to breach the School's policies;

21.1.6 protect members of the school community, public and private property; and

21.1.7 assist in managing the School.

21.2 Please refer to the School's CCTV Policy for more information.

22. Policy Review

22.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

22.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

23. Enquiries

23.1 Further information about the School's Data Protection Policy is available from the DPO.

23.2 General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Document Control

Date modified	Description of modification	Modified by

Appendix 1 – UK GDPR Clauses

The UK GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the UK GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))
2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))
3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)
4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))
5. The Processor must ensure it flows down the UK GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))
6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3)(e))
7. The Processor must assist the Data Controller with their security and data breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))
8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))
9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under UK law. (Art. 28(3)(g))
10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))

11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach UK law. (Art. 28(3))

Appendix 2 – Privacy Notices

1) Student Privacy Notice
2) Parents Privacy Notice
3) Staff and Governors Privacy Notice

PRIVACY NOTICE FOR STUDENTS ATTENDING RICKMANSWORTH SCHOOL

Rickmansworth School collects a lot of data and information about our students so that we can run effectively as a school. This privacy notice explains how and why we collect students' data, what we do with it and what rights parents and students have.

Privacy Notice (How we use student information)

Rickmansworth School is a popular oversubscribed academy. The number on roll is 1,385. Our Data Protection Officer is Matthew Lantos and his email is DPO@rickmansworth.herts.sch.uk

Why do we collect and use student information?

We collect and use student information under the following lawful bases:

a. where we have the consent of the data subject (Article 6 (a));

b. where it is necessary for compliance with a legal obligation (Article 6 (c));

c. where processing is necessary to protect the vital interests of the data subject or another person (Article 6(d));

d. where it 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 (Article 6 (e)).

Where the personal data we collect about students is Special Category data, we will only process it where:

a. we have explicit consent;

b. 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; and / or

c. processing is necessary for reasons of substantial public interest, on the basis of UK 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.

Please see our Data Protection Policy for a definition of Special Category Data.

We use the student data to support our statutory functions of running a school, in particular:

a. to decide who to admit to the school;
b. to maintain a waiting list;

c. to support student learning;
d. to monitor and report on student progress;
e. to provide appropriate pastoral care;
f. to assess the quality of our services;
g. to comply with the law regarding data sharing;
h. for the protection and welfare of students and others in the school;
i. for the safe and orderly running of the school;
j. to promote the school;
k. to communicate with parents / carers.

The categories of student information that we collect, hold and share include:

a. Personal information (such as name, unique student number and address);
b. Characteristics (such as ethnicity, language, medical conditions, nationality, country of birth and free school meal eligibility);
c. Attendance information (such as sessions attended, number of absences and absence reasons)
d. Biometric Information (such as partial fingerprints for cashless catering and audio/visual image for remote learning)

From time to time and in certain circumstances, we might also process personal data about students, some of which might be Special Category data, including information about criminal proceedings / convictions, information about sex life and sexual orientation, child protection / safeguarding. This information is not routinely collected about students and is only likely to be processed by the school in specific circumstances relating to particular students, for example, if a child protection issue arises or if a student is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

We collect information about students when they join the school and update it during their time on the roll as and when new information is acquired.

As the school has a cashless catering system, we also process biometric data about students. Please see our Data Protection Policy for more details about how we process biometric data.

As part of our remote learning solution through Google Classroom we may also record your video image and voice. In addition, if you access the system from home, we will also hold information on your IP address, device details and device Operating System.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK General Data Protection Regulation ('**UK GDPR**'), the Data Protection Act 2018 ('**DPA**'), and other regulations (together 'the **UK Data Protection Legislation**'), we will inform you whether you are required to provide certain student information to us or if you have a choice in this. Where appropriate, we will ask parents / students for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to use photos or images of students on our website or on social media to promote school activities or if we want to ask your permission to use your information for marketing purposes. Parents / students may withdraw consent at any time.

For secondary schools: When students are deemed to be old enough to make their own decisions in relation to their personal data, we will also ask the student for their consent in these circumstances. This will usually be around the age of 13. Although parental consent is unlikely to be needed, we wish to take a collaborative approach so we will keep parents informed when we are approaching students for consent up to the age of 18. Students with the maturity to make their own decisions about their personal data may withdraw consent if consent has previously been given.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or investigate other issues. CCTV footage involving students will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

A significant amount of personal data is stored electronically, for example, on our MIS database. Some information may also be stored in hard copy format.

Data stored electronically may be saved on a cloud based system which may be hosted in a different country.

Personal data may be transferred to other countries if, for example, we are arranging a school trip to a different country. Appropriate steps will be taken to keep the data secure.

Who do we share student information with?

We routinely share student information with:

- schools that students attend after leaving us;
- our local authority Hertfordshire County Council;
- a student's home local authority (if different);
- the Department for Education (DfE);
- school governors / trustees;

- exam boards.

From time to time, we may also share student information other third parties including the following:

- the Police and law enforcement agencies;
- NHS health professionals including the school nurse, educational psychologists,
- Education Welfare Officers;
- Courts, if ordered to do so;
- the National College for Teaching and Learning;
- the Joint Council for Qualifications;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances;
- our HR providers, for example, if we are seeking HR advice and a student is involved in an issue;
- UCAS
- our legal advisors;
- our insurance providers

Some of the above organisations may also be Data Controllers in their own right in which case we will be jointly controllers of your personal data and may be jointly liable in the event of any data breaches.

In the event that we share personal data about students with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

Why we share student information

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

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

Data collection requirements:

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

Youth support services

What is different about students aged 13+?

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent / guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Our students aged 16+We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services;
- careers advisers.

For more information about services for young people, please visit our local authority website.

The National Student Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the student information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to store and handle the data.

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

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

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-student-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

For secondary schools: Under data protection legislation, students, and in some circumstances, parents, have the right to request access to information about them that we hold ("Subject Access Request"). From the age of 13, we generally regard students as having the capacity to exercise their own rights in relation to their personal data. This means that where we consider a student to have sufficient maturity to understand their own rights, we will require a Subject Access Request to be made by the student and not their parent(s) on their behalf. This does not affect any separate statutory right parents might have to access information about their child.

For all schools: Subject to the section below, the legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage parents / students to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our Data Protection Policy.

For academies: Parents of students who attend academies have a separate statutory right to receive an annual written report setting out their child's attainment for the main subject areas which are taught. This is an independent legal right of parents rather than a student's own legal right which falls outside of the UK GDPR, therefore a student's consent is not required even if a student is able to make their own decisions in relation to their personal data, unless a court order is in place which states otherwise.

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the student, with whom the student lives or whether the student has contact with that parent), and also includes non-parents who have parental responsibility for the student, or with whom the student lives. It is therefore possible for a student to have several "parents" for the purposes of education law.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of our data protection responsibilities.

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

Contact:
If you would like to discuss anything in this privacy notice, please contact:

Matthew Lantos
Data Protection Officer (DPO)
DPO@rickmansworth.herts.sch.uk

PRIVACY NOTICE FOR PARENTS / CARERS OF STUDENTS ATTENDING RICKMANSWORTH SCHOOL

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the student, with whom the student lives or whether the student has contact with that parent), and also includes non-parents who have parental responsibility for the student, or with whom the student lives. It is therefore possible for a student to have several "parents" for the purposes of education law. This privacy notice also covers other members of students' families who we may process data about from time to time, including, for example, siblings, aunts and uncles and grandparents.

Privacy Notice (How we use parent / carer information)

Rickmansworth School is a popular, oversubscribed Academy. It has a mixed intake of 1,385.

Why do we collect and use parent / carer information?

Our Data Protection Officer is Matthew Lantos and his email address is DPO@rickmansworth.herts.sch.uk

We collect and use parent / carer information under the following lawful bases:

a. where we have the consent of the data subject (Article 6 (a));

b. where it is necessary for compliance with a legal obligation (Article 6 (c));

c. where processing is necessary to protect the vital interests of the data subject or another person (Article 6(d));

d. where it 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 (Article 6 (e)).

Where the personal data we collect about parents / carers is Special Category data, we will only process it where:

a. we have explicit consent;

b. 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; and / or

c. processing is necessary for reasons of substantial public interest, on the basis of UK law which shall be proportionate to the aim pursued, where we 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.

Please see our Data Protection Policy for a definition of Special Category data.

We use the parent / carer data to support our functions of running a school, in particular:

a. to decide who to admit to the school;
b. to maintain a waiting list;
c. to support student learning;
d. to monitor and report on student progress;
e. to provide appropriate pastoral care;
f. to assess the quality of our services;
g. to comply with the law regarding data sharing;
h. for the protection and welfare of students and others in the school, including our safeguarding / child protection obligations;
i. for the safe and orderly running of the school;
j. to promote the school;
k. to send you communications that may be of interest to you which may include information about school events or activities, news, campaigns, appeals, other fundraising activities;
l. in order to respond to investigations from our regulators or to respond to complaints raised by our stakeholders;
m. in connection with any legal proceedings threatened or commenced against the school.

The categories of parent / carer information that we collect, hold and share include:

a. Personal information (such as name, address, telephone number and email address);

b. Information relating to your identity, marital status, employment status, religion, ethnicity, language, medical conditions, nationality, country of birth and free school meal / student premium eligibility / entitlement to certain

benefits, information about court orders in place affecting parenting arrangements for students);

From time to time and in certain circumstances, we might also process personal data about parents / carers, some of which might be Special Category data, information about criminal proceedings / convictions or information about child protection / safeguarding. This information is not routinely collected about parents / carers and is only likely to be processed by the school in specific circumstances relating to particular students, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

We collect information about parents / carers before students join the school and update it during students' time on the roll as and when new information is acquired.

Collecting parent / carer information

Whilst the majority of information about parents / carers provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain parent / carer information to us or if you have a choice in this. Where appropriate, we will ask parents / carers for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to ask your permission to use your information for marketing purposes or to request voluntary contributions. Parents / carers may withdraw consent given in these circumstances at any time.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or investigate other issues. CCTV footage involving parents / carers will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

Storing parent / carer data

A significant amount of personal data is stored electronically, for example, on our MIS database. Some information may also be stored in hard copy format.

Data stored electronically may be saved on a cloud based system which may be hosted in a different country.

Personal data may be transferred to other countries if, for example, we are arranging a school trip to a different country. Appropriate steps will be taken to keep the data secure.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer a parent / carer we will retain and securely destroy your personal information in accordance with our data retention policy.

Who do we share parent / carer information with?

We routinely share parent / carer information with:

- schools that students attend after leaving us

From time to time, we may also share parent / carer information other third parties including the following:

- our local authority Hertfordshire County Council;
- a student's home local authority (if different);
- the Department for Education (DfE);
- school governors / trustees;
- the Police and law enforcement agencies;
- NHS health professionals including the school nurse, educational psychologists,
- Education Welfare Officers;
- Courts, if ordered to do so;
- the Teaching Regulation Authority;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances;
- UCAS
- our legal advisors;
- our insurance providers / the Risk Protection Arrangement;

Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

In the event that we share personal data about parents / carers with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

Requesting access to your personal data

Under data protection legislation, parents / carers have the right to request access to information about them that we hold. To make a request for your child's personal data, or be given access to your child's educational record, contact dpo@rickmansworth.herts.sch.uk although any written request for personal data will be treated as a Subject Access Request. A majority of online data is on SIMS for which parents/carers already have access.

The legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage parents / carers to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of our data protection responsibilities.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To

withdraw your consent, please contact the Data Team. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

DATA PROTECTION OFFICER

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO Mr Matthew Lantos, DPO@rickmansworth.herts.sch.uk. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

PRIVACY NOTICE FOR STAFF AND GOVERNORS

WHAT IS THE PURPOSE OF THIS DOCUMENT?

Rickmansworth School is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you before, during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

It applies to all employees, workers, governors and contractors.

Rickmansworth School is a popular 11-18 mixed Academy.

The Data Protection Officer is Matthew Lantos, DPO@rickmansworth.herts.sch.uk

Rickmansworth School is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other type of contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

1. DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

(a) Used lawfully, fairly and in a transparent way.

(b) Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

(c) Relevant to the purposes we have told you about and limited only to those purposes.

(d) Accurate and kept up to date.

(e) Kept only as long as necessary for the purposes we have told you about.

(f) Kept securely.

2. THE TYPE OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth

- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Teacher Reference Number
- Start date
- Location of employment or workplace
- Copy of driving licence
- Recruitment information (including copies of pre-vetting recruitment and identity checks (including, where appropriate, information about your employment history, Standard or Enhanced Disclosure and Barring Service Checks, Barred Lists Checks, prohibition checks/section 128 checks and disqualification checks, for example under the Childcare (Disqualification) Regulations 2009 and any further checks that are required if you have lived or worked outside the UK), your nationality and right to work documentation, references and other information included in a CV, application form or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Performance information
- Disciplinary and grievance information, including warnings issued to you
- CCTV footage and other information obtained through electronic means such as swipe card records
- Information about your use of our information and communications systems
- Photographs

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Information about your health, including any medical condition, health and sickness records
- Genetic information and biometric data
- Information about your criminal record

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the Local Authority or other background check agencies.

We will also collect additional personal information in the course of job-related activities throughout the period of you working for us.

3. HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

(a) Where we need to perform the contract we have entered into with you.

(b) Where we need to comply with a legal obligation.

We may also use your personal information in the following situations:

(c) Where we need to protect your interests (or someone else's interests).

(d) Where it is needed in the public interest or for official purposes.

4. Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you, to enable us to comply with legal obligations and/or where it is needed in the public interest or for official purposes. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us

- Checking you are legally entitled to work in the UK
- Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working in specific positions via the Teacher Services Online platform
- To maintain our single central record and to comply with our general safeguarding obligations
- To provide information on our website for carers/leavers
- Where appropriate, to disclose certain information in the Academy's accounts in accordance with the Accounts direction
- Paying you and, if you are an employee, deducting tax and National Insurance contributions
- Providing the following benefits to you: Child care vouchers, Cycle Scheme, Eye Tests
- Liaising with your pension provider
- Administering the contract, we have entered into with you
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Responding to complaints or investigations from stakeholders or our regulators
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Providing references to prospective employers
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work

- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- To maintain and promote equality in the workplace
- To receive advice from external advisors and consultants
- In appropriate circumstances to liaise with regulatory bodies, such as the Department for Education, the DBS and the Local Authority about your suitability to work in a school or in connection with other regulatory matters

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or investigate other issues. CCTV footage involving staff will only be processed to the extent that it is lawful to do so.

5. If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers) or we may be unable to discharge our obligations which may be in the public interest or for official purposes.

6. Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal

information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

7. HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require us to ensure higher levels of data protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

(e) In limited circumstances, with your explicit written consent.

(f) Where we need to carry out our legal obligations

(g) Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Data Protection Policy.

(h) Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

8. Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence including the reasons for the leave, which may include sickness absence or family-related leave, sabbaticals, to comply with employment and other laws.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to comply with the Equality Act 2010, to monitor and manage sickness absence and to administer benefits.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual

orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use your particularly sensitive information in accordance with our written policy where processing is necessary:

- to carry out our legal obligations or exercise specific rights in the field of employment law;
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- for reasons of substantial public interest, on the basis of UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and we provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In other circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract of employment with us that you agree to any request for consent from us.

9. INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we

will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

· Risk Assess an individual

· To take Human Resources advice.

10. AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

(i) Where we have notified you of the decision and given you 21 days to request a reconsideration.

(j) Where it is necessary to meet our obligations under your employment contract and ensure that appropriate measures are in place to safeguard your rights.

(k) In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

11. DATA SHARING

We may have to share your data with third parties, including third-party service providers and other organisations.

In particular, we may share your data with organisations including, but not limited to, the following:

- the Local Authority
- the Department for Education
- the Education & Skills Funding Agency
- the Disclosure and Barring Service

- the Teaching Regulation Agency
- the Teachers' Pension Service
- the Local Government Pension Scheme
- our external HR provider
- our external payroll provider
- HMRC
- the Police or other law enforcement agencies
- our legal advisors
- insurance providers

We require third parties to respect the security of your data and to treat it in accordance with the law. Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

We may transfer your personal information outside the UK. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might we share your personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, where it is needed in the public interest or for official purposes, or where we have your consent.

Which third-party service providers process your personal information?

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services.

12. Department for Education

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

For use by academies and free schools only: We are required to share information about our students with the Department for Education (DfE) under regulation 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 as amended.

13. DfE data collection requirements

The following is information provided by the DfE concerning the reason it collects data about school employees:

- The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Student Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

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

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff by:

- conducting research or analysis;
- producing statistics; and / or
- providing information, advice or guidance

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with the

DfE's strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data To contact the department: https://www.gov.uk/contact-dfe

How secure is your information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible joining with another Multi Academy Trust. We may also need to share your personal information with a regulator or to otherwise comply with the law.

From time to time, we may disclose your personal data in response to a request for information pursuant to the Freedom of Information Act 2000 or following a data subject access request. We may approach you for your consent but, in any event, we will only disclose your personal data if we are satisfied that it is reasonable to do so in all the circumstances. This means that we may refuse to disclose some or all of your personal data following receipt of such a request.

14. Transferring information outside the UK

We may sometimes transfer your personal data outside of the UK if, for example, we are arranging a school trip and we are booking transport, accommodation or activities. In these circumstances, we will obtain your consent for us to process your data in this way.

15. DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are available.

Third parties who are processing personal data on our behalf will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

16. DATA RETENTION

How long will we use your information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. (Details of retention periods for different aspects of your personal information are available in our Data Retention Policy). To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

17. RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

18. Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (data subject access request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete

or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Deputy Head in writing.

The legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage data subjects to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. (For further information about how we handle Subject Access Requests, please see our Data Protection Policy).

19. No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

20. What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

21. RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the SLT Lead for Data

Protection. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

22. DATA PROTECTION OFFICER

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

You can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

23. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the SLT Lead for Data Protection.