Data Protection Policy

Firthmoor Primary School

Document Version Control				
Document Type:		POLICY		
Document Author:		**IT Systems & Support Limited**		
Document Owner:		Data Protection Officer		
Document Security Classification:		PUBLIC		
Document Review Period:		ANNUAL		
Issue	**Description of Changes**	**Changer**	**Authoriser**	**Issue Date**
1.0	Initial Draft	Tristen Coad	Amie Chambers	31/01/2024
1.1	Annual Review: - Removal legacy documentation naming convention - Creation of aims introduction - Incorporation of KCSIE updates - Incorporation of statutory requirements - Further expansion of data types - Updates applied to: o Consent o Data Protection Principles o Data Subject Rights o Data Types o Transfers of Personal Data o Data Protection CPD o Privacy Procedure	Tristen Coad	Amie Chambers	31/01/2025

Considerations, Definitions & Terms	
School	Nursery, School, Academy, Trust, College, SAT, MAT
Learner	Pupil, Student, Child, Children
Parent	Parent, Guardian, Person(s) of care, holder of parental responsibility, Person in Parental Responsibility for a Learner
Office Manager	Administrative Lead, School/Trust Business Manager, Administrative Manager
Headteacher	Headteacher, Principal, CEO, Deputy CEO, Executive Headteacher, Head of School
Senior Leader	Any and all members of Senior Leadership Team / Executive Leadership Team

Introduction

1.1 The aims of this policy are to provide a single portfolio for all persons to understand:

1.1.1 Data protection law in relation to **The School;**

1.1.2 How **The School** is enacting data protection law in its everyday role as an education provider; and

1.1.3 How **The School** is upholding the rights and freedoms of all directly and indirectly persons affected by data protection rules in its role as an education provider.

1.2 Both the UK Data Protection Act 2018 and UK GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe and promoting their welfare. If in any doubt about sharing information, staff should speak to the designated safeguarding lead. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children. Information relating to information sharing and safeguarding can be found on the UK Department for Education (DfE) web page:- https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.3 Under UK GDPR it is a statutory requirement for **The School** to have a Data Protection Policy which can be found:

1.3.1 For Academies - https://www.gov.uk/guidance/-governance-in-academy-trusts/statutory-policies-for-trusts

1.3.2 For maintained schools - https://www.gov.uk/guidance/governance-in-maintained-schools/statutory-policies-for-maintained-schools

2. Definitions

2.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2021 replaces the UK Data Protection Directive of 1995 and supersedes laws that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

2.2 Definitions used by the organisation (drawn from the GDPR)

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

Territorial scope (Article 3) **–** the GDPR will apply to all controllers that are established in the UK who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the UK that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the UK.

2.3 Article 4 definitions

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

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

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

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

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

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

Personal data breach **–** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to

report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

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

Child **–** the GDPR defines a child as anyone under the age of 13 by UK law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by **The Parent**. Children under the age of 13 are not usually considered able to give consent to process data or to directly access the rights of a data subject. **The Parent** is able to undertake this role providing this is in the best interests of the child. Children should be provided with age appropriate advice about how their data is used.

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

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

3. Policy statement

3.1 The Governing Body and management of «SITE_NAME», are committed to compliance with all relevant UK law in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information **The School** collects and processes in accordance with the General Data Protection Regulation (GDPR).

3.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

3.3 The GDPR and this policy apply to all of **The School** personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

3.4 **The School** has established objectives for data protection and privacy.

3.5 The Data Protection Officer (DPO) / GDPR Owner is responsible for reviewing the register of processing annually in the light of any changes to **The School** activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

3.6 This policy applies to all Employees and interested parties of **The School** such as outsourced suppliers. Any breach of the GDPR or this PIMS will be dealt with under **The School** disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

3.7 Partners and any third parties working with or for **The School**, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by **The School** without having first entered into a data confidentiality agreement as part of our contractual service level agreement, which imposes on the third party obligations no less onerous than those to which **The School** is committed, and which gives **The School** the right to audit compliance with the agreement.

Personal information management system (PIMS)

Policy statement

To support compliance with the GDPR, the Governing Body has approved and supported the development, implementation, maintenance and continual improvement of a documented personal information management system ('PIMS') for **The School**.

All Employees of **The School** and certain external parties identified in the PIMS are expected to comply with this policy and with the PIMS that implements this policy. All Employees, and certain external parties, will receive and be required to provide appropriate training. The consequences of breaching this policy are set out in **The School** disciplinary policy and in contracts and agreements with third parties.

In determining its scope for compliance with the GDPR, **The School** considers:

- any external and internal issues that are relevant to the purpose of **The School** and that affect its ability to achieve the intended outcomes of its PIMS;
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS;
- organisational objectives and obligations;
- the organisations acceptable level of risk; and
- any applicable statutory, regulatory or contractual obligations.

The School objectives for compliance with the GDPR and a PIMS:

- are consistent with this policy
- are measurable
- take into account GDPR and the results from risk assessments and risk treatments
- are monitored
- are communicated
- are updated as appropriate

In order to achieve these objectives, **The School** has determined:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated

Responsibilities and roles under the General Data Protection Regulation

3.8 **The School** is a data controller and data processor under the GDPR.

3.9 Top Management and all those in managerial or supervisory roles throughout **The School** are responsible for developing and encouraging good information handling practices within **The School**; responsibilities are set out in individual job descriptions.

3.10 Data Protection Officer (DPO), a role specified in the GDPR, should be a member of the senior management team, is accountable to the Governing Body of **The School** for the management of personal data within **The School** and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.10.1 development and implementation of the GDPR as required by this policy; and

3.10.2 security and risk management in relation to compliance with the policy.

3.11 Data Protection Officer (DPO), who the Governing Body considers to be suitably qualified and experienced, has been appointed to take responsibility for **The School** compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that **The School** complies with the GDPR, as do Manager's in respect of data processing that takes place within their area of responsibility.

3.12 The Data Protection Officer (DPO) has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

3.13 Compliance with data protection legislation is the responsibility of all Employees of **The School** who process personal data.

3.14 **The School** Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees of **The School** generally.

3.15 Employees of **The School** are responsible for ensuring that any personal data about them and supplied by them to **The School** is accurate and up-to-date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. **The School** policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing" and include:

4.1.1 Given consent (Article 6, 1a)
4.1.2 Contractual obligation (Article 6, 1b)
4.1.3 Legal obligation (Article 6, 1c)
4.1.4 In the vital interest(s) of the data subject(s) (Article 6, 1d)
4.1.5 In the public interest(s) (Article 6, 1e)
4.1.6 In the legitimate interest(s) of the controller / third-party (Article 6, 1f)

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.
The School Privacy Notice Procedure is set out in the Privacy Notice Policy.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.7 the identity and the contact details of the controller and, if any, of the controller's representative;
4.1.8 the contact details of the Data Protection Officer (DPO);
4.1.9 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.10 the period for which the personal data will be stored;
4.1.11 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.1.12 the categories of personal data concerned;
4.1.13 the recipients or categories of recipients of the personal data, where applicable;
4.1.14 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
4.1.15 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of **The School** GDPR register of processing. Privacy Procedure GDPR DOC 2.1 sets out the relevant procedures.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 The Data Protection Officer (DPO) is responsible for ensuring that **The School** does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer (DPO).

4.3.3 The Data Protection Officer (DPO) will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The Data Protection Officer (DPO) is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by **The School** is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4 Employees/Staff should be required to notify **The School** of any changes in circumstance to enable personal records to be updated accordingly. Employees/Staff are required to contact the senior administrative staff and obtain a data collection/correction form for completion. It is the responsibility of **The School** to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The Data Protection Officer (DPO) is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On at least an annual basis, the Data Protection Officer (DPO) will review the retention dates of all the personal data processed by **The School**, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

4.4.7 The Data Protection Officer (DPO) is responsible for responding to requests for rectification from data subjects (subject to proof of ID and change) within one month. This can be extended to a further two months for complex requests. If

The School decides not to comply with the request, the Data Protection Officer (DPO) must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

4.4.8 The Data Protection Officer (DPO) is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.5.1 Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

4.5.2 Personal data will be retained in line with the statutory Retention of Records and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

4.5.3 The Data Protection Officer (DPO) must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure (GDPR DOC 2.3), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security

The Data Protection Officer (DPO) will carry out a risk assessment taking into account all the circumstances of **The School** controlling or processing operations.

In determining appropriateness, the Data Protection Officer (DPO) should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on **The School** itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer (DPO) will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to **The School**.

When assessing appropriate organisational measures the Data Protection Officer (DPO) will consider the following:

- The appropriate training levels throughout **The School**;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the UK.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The School compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the information security policy.

4.7 <u>The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)</u>

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

The School will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 5.1.2 To prevent processing likely to cause damage or distress.
- 5.1.3 To prevent processing for purposes of direct marketing.
- 5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 5.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
- 5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- 5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- 5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 5.1.10 To object to any automated profiling that is occurring without consent.

5.2 **The School** ensures that data subjects may exercise these rights:

- 5.2.1 Ensuring data subjects are aware of their rights under GDPR for:
  - 5.2.1.1 The right to be informed (Articles 13 and 14);
  - 5.2.1.2 The right of access (Article 15);
  - 5.2.1.3 The right to rectification (Article 16);
  - 5.2.1.4 The right to erasure (Article 17);
  - 5.2.1.5 The right to restrict processing (Articles 18 and 19);
  - 5.2.1.6 The right to data portability (Article 20);
  - 5.2.1.7 The right to object (Article 21); and
  - 5.2.1.8 Rights in relation to automated decision making and profiling (Article 22).
- 5.2.2 Data subjects may make data access requests as described in Subject Access Request (SAR) Procedure; this procedure also describes how **The School** will ensure that its response to the data access request complies with the requirements of the GDPR.
- 5.2.3 UK GDPR gives individuals the right to access any data that an organisation holds on them. A SAR must be completed within 30 calendar days without charge to the data subject.
- 5.2.4 Schools should be aware that guidance from the ICO highlights the rights of the child. "Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow **The**

Parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child."

5.2.5 Under the Education (Pupil Information England) Regulations 2005 **The Parent** has statutory rights to access and obtain a copy of **The Learners** education record. This sits outside of the UK GDPR schedule and must be completed within 15 working days:- https://ico.org.uk/for-the-public/schools/pupils-info/

5.2.6 Data subjects have the right to complain to **The School** related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the School Complaints Procedure.

5.2.7 Under Article 17 of the UK GDPR data subjects have the right to have their personal data erased; the 'right to be forgotten'. This right applies to all data held at the time and does not apply to any potential future data that may be created in the future. In regards to **The Learner's** data, emphasis must be given on the following aspects which considering an erasure request from **The Parent** due to the enhanced protection of children's information.

5.2.8 There may be occasions when the right of access and right of erasure do not apply and can be refused. These can include, but not limited to:

- 5.2.8.1 to comply with a legal and/or statutory obligation;
- 5.2.8.2 for the performance of a task in the public interest;
- 5.2.8.3 necessary for public health purposes;
- 5.2.8.4 the establishment, exercise or defence of a legal claim;
- 5.2.8.5 where there is a potential risk to the health and wellbeing of the data subject; and
- 5.2.8.6 where " it is likely to cause significant harm to the physical or mental health of the child or others" – DfE KCSIE.

6. Data Types

6.1 The ICO defines personal data as "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."

6.2 Under Article 9, Section 1 of the UK GDPR it is prohibited to process "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." **The School** is authorised to process special categories of data under Section 2 of Article 9 for legal, statutory, vital interest, and in the public interest. Explicit consent can also be sought for processing this level of data should it be required to undertake explicit processing of sensitive data.

7. Consent

7.1 **The School** understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

7.2 **The School** understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

7.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

7.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.5 In most instances, consent to process personal and sensitive data is obtained routinely by **The School** using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

7.6 Where **The School** provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of

16 (unless the UK has made provision for a lower age limit, which may be no lower than 13).

8. Security of data

8.1 All Employees/Staff are responsible for ensuring that any personal data that **The School** holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by **The School** to receive that information and has entered into a confidentiality agreement as part of their contractual service level agreement.

8.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

8.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of **The School**. All Employees are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

8.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with Secure Disposal of Storage Media.

8.5 Personal data may only be deleted or disposed of in line with the Retention of Records. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

8.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

9. Disclosure of data

9.1 **The School** must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of **The School** business.

9.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer (DPO).

10. Privacy Procedures and Notices

10.1 The Data Protection Officer (DPO) is responsible for ensuring that Privacy Notices are correct and that mechanisms exist such as having the Privacy Notice(s) accessible in a public, machine-readable format allowing data subjects aware of all matter relating to data collection and processing by **The School**.

10.2 **The School** identifies the basis for processing personal data before any processing operations take place. This information must be recorded in line with a Data Protection Impact Assessment (DPIA) by clearly establishing, defining and documenting:

10.2.1 the specific purpose of processing the personal data and the basis to process the data; and

10.2.2 any special categories of personal data processed and the basis to process the data.

10.3 Should personal data be collected from data subject with consent **The School** must be transparent in its processing of personal data and provides the data subject with the following:

10.3.1 The identity, and contact details of the Data Protection Officer (DPO) and any data protection representatives;

10.3.2 The purpose(s) for the intended processing of personal data;

10.3.3 Potential recipients of the personal data;

10.3.4 Any information regarding the intention to disclose personal data to third parties and whether it is transferred outside the UK. In such circumstances, **The School** will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards;

10.3.5 Any information on technologies used to collect personal data about the data subject;

10.3.6 Any other information required to demonstrate that the processing is fair and transparent such as:

10.3.6.1.1 Retention

10.3.6.1.2 Data subjects right to access

10.3.6.1.3 Right to lodge complaint

10.3.6.1.4 Right to withdraw consent

10.4 All information provided to the data subject must be in an easily accessible format, using clear and plain language, especially for personal data addressed to a child.

10.5 Data which is legally and/or contractually required for processing must be recorded in **The School's** Privacy Notice.

11. Retention and disposal of data

11.1 **The School** shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

11.2 **The School** may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

11.3 The retention period for each category of personal data will be set out in the Retention of Records along with the criteria used to determine this period including any statutory obligations **The School** has to retain the data.

11.4 **The School** data retention and data disposal procedures will apply in all cases.

11.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

12. Data transfers

12.1 All exports of data from the UK to non-UK countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the UK is prohibited unless one or more of the specified safeguards, or exceptions, apply:

12.1.1 An adequacy decision

The UK can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

12.1.2 Privacy Shield

If **The School** wishes to transfer personal data from the UK to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to a UK resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the UK under that framework.

<u>Assessment of adequacy by the data controller</u>

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

12.1.3 Binding corporate rules

The School may adopt approved binding corporate rules for the transfer of data outside the UK. This requires submission to the relevant supervisory authority for approval of the rules that **The School** is seeking to rely upon.

12.1.4 <u>Model contract clauses</u>

The School may adopt approved model contract clauses for the transfer of data outside of the UK. If **The School** adopts the there is an automatic recognition of adequacy.

12.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

13. Data Protection Training and CPD

13.1 The Data Protection Officer (DPO) shall ensure that all Staff with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, demonstrate compliance with the GDPR.

13.2 These members of Staff must be able to demonstrate competence in their understanding of the GDPR, how this is practised and implemented throughout The School.

13.3 The Data Protection Officer (DPO) ensures that these members of Staff are kept up to date and informed of any issues related to personal data.

13.4 Governing Body promote training and awareness programmes, and The School shall make resources available in order to raise awareness. The Data Protection Officer (DPO) shall demonstrate and communicate to Staff the importance of data protection in their role and ensure that they understand how and why personal data is processed in accordance with The School policies and procedures.

13.5 All employees of The School, paid or voluntary, are provided with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with The School policies and procedures.

13.6 Staff are provided with specific training on any information security requirements and procedures applicable to data protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal data breaches.

13.7 Staff are provided with training on dealing with complaints relating to data protection and processing personal data.

13.8 The Office Manager and Data Protection Officer (DPO) will retain records of the relevant training undertaken by each person who has this level of responsibility.

13.9 The Data Protection Officer (DPO) and Office Manager are responsible for organising relevant training for all responsible individuals and Staff generally, and for maintaining records of the attendance of staff at relevant training at appropriate times across The School business cycle.

14. Information asset register/data inventory

14.1 **The School** has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. **The School** data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

14.2 **The School** is aware of any risks associated with the processing of particular types of personal data.

14.2.1 **The School** assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) (DPIA Procedure) are carried out in relation to the processing of personal data by **The School**, and in relation to processing undertaken by other organisations on behalf of **The School**.

14.2.2 **The School** shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

14.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, **The School** shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

14.2.4 Where, as a result of a DPIA it is clear that **The School** is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not **The School** may proceed must be escalated for review to the Data Protection Officer (DPO).

14.2.5 The Data Protection Officer (DPO) shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

14.2.6 Appropriate controls will be selected from Annex A of ISO 27001 and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to **The School** documented risk acceptance criteria and the requirements of the GDPR.