ST HERBERT'S CE PRIMARY AND NURSERY SCHOOL

DATA PROTECTION POLICY

2025/2027

Approved by[1]			
Name:	Full Governing Body		
Date:	7th July 2025	**Version No:**	
Proposed review date[2]**:**	July 2027		

[1] The Governing Body is free to determine how to implement this policy. Obtain further advice from the Information Commissioner's Office website www.ico.org.uk.

[2] This document should be reviewed at least every two years

REVIEW SHEET

Each entry in the table below summarises the changes to this Policy made since the last review (if any).

Version Number	Version Description	Date of Revision
1	Original	March 2012
2	Minor changes to Privacy Notices	July 2012
3	Changes Highlighted.	November 2012
4	Reformatted only	February 2014
5	Updated to take account of the DfE model Privacy Notices issued July 2014. NOTE: Appendices C and D have been amalgamated.	July 2014
6	Minor revisions and contact detail changes only to Privacy Notices	July 2015
7	Updated Privacy Notices	December 2016
8	Updated Privacy Notices in line with the GDPR.	October 2017
9	Updated Privacy Notices to reflect DfE revised models published January 2018.	January 2018
10	Major re-write to comply with GDPR	May 2018
11	Review/Update	June 2021
12	Review/Update	July 2023
13	Review/Update	July 2025

Contents

1. Introduction 1
1.1 Policy purpose 1
1.2 Policy scope and definitions 1
2. Roles and responsibilities 3
3. Data protection principles 3
3.1 Conditions for the lawful processing of personal data 4
3.2 Conditions for the lawful processing of special categories of data 5
3.3 Deciding which condition to rely on 6
3.4 Privacy Notices 6
4. Individuals' rights and how we protect them 6
4.1 The right to be informed about the collection and use of their personal data 7
4.2 The right of access to their personal data and relevant supplementary information 7
4.3 The right to rectification if the information held is inaccurate or incomplete 7
4.4 The right to erasure of personal data 7
4.5 The right to restrict the processing of personal data 9
4.6 The right to data portability 9
4.7 The right to object to processing 10
4.8 The right to object to automated decision making and profiling 10
5. Subject Access Requests (SARs) 10
6. Data protection and privacy by design 11
6.1 Data Protection Impact Assessments (DPIAs) 12
7. Training & Awareness 12
8. Publication of Information 13
9. Managing Consent 13
9.1 Consent to use personal data including images and voice recordings 13
9.2 Consent for the use of generative artificial intelligence (intellectual property) 15
9.3 Data sharing during a public health emergency: consent and data retention 15
10. Data Security and Integrity 16
10.1 Classification of data 16
10.2 Organisational and technical security measures 17
10.3 Email 18
10.4 Generative Artificial Intelligence 18
10.5 Transfers of data outside the UK 19
10.6 Record keeping 19
11. Data Sharing 20
12. Data Retention 20
13. Data Disposal 20
14. Breach Reporting 21
15. Our Obligations to our Data Processors 21
Appendix A Data Classifications and Handling Requirements Table
Appendix B Privacy Notice for Pupils

Appendix C Privacy Notice for School Workforce
Appendix D privacy Notice for Governors
Appendix E Privacy Notice for Visitors

1. Introduction

The Data Protection Act 2018 provides a legal framework for data protection in the United Kingdom (UK). It incorporates the General Data Protection Regulations (GDPR), the legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) and is sometimes referred to as UK GDPR.

UK GDPR significantly updates previous Data Protection law to reflect changes in technology and the way organisations collect and use information about people in the 21st century. It regulates the processing of personal data and gives rights of privacy protection to all living persons.

In accordance with the DPA, we at St Herbert's CE Primary and Nursery School recognise that we collect and process personal data and because we decide how and why we do that, we are *data controllers*. This means that we have legal obligations to people regarding how we handle their data and manage their privacy and we must register as a data controller with the Information Commissioner's Office (ICO). Anyone can read the details of our ICO notification by going online to https://ico.org.uk/esdwebpages/search and entering our registration number. Data controllers are normally organisations and not people although our Head teacher is responsible for everything we do day-to-day and we have appointed a Data Protection Officer (DPO).

Our ICO Registration Number is: Z7449612.

Our Data Protection Officer is: Reverend Charles Hope.

Contact our DPO on 017687 73017 or email them at: dpo@stherberts.cumbria.sch.uk

We recognise that when we process personal data it can involve collecting, recording, organising, storing, altering, retrieving, using, disclosing, restricting, and erasing or destroying it, and there can be risks associated with that processing to the people whose data it is. Failure to adequately protect people's personal information can result in significant, even life-changing harm to some individuals, distress, loss of public trust in us, and legal repercussions including fines and other sanctions.

The DfE provides access to a Data Protection toolkit for schools and we will make use of that toolkit as necessary

1.1 Policy purpose

Through this policy we aim to ensure that current and future pupils, staff, volunteers, and other partner organisations can feel confident that our school is a safe and secure place to learn or work, and to demonstrate our commitment to protecting the rights and privacy of everyone whose data we handle by setting out:

- our obligations in the context of what we do.
- clear roles, responsibilities, reporting, and management structures aimed at protecting people's personal data and their rights.
- clear procedures for handling data to achieve our aim of taking reasonable and proportionate steps to protect people.

1.2 Policy scope and definitions

This policy applies to all governors, trustees, staff, and volunteers who handle or have access to personal data regardless of where they are physically working e.g., at home, at another organisation, on trips, and to all personal information processed by us or on our behalf. This includes the personal information of our data subjects accessed or used by other organisations which work for or with us e.g., Local Authority workers, contractors, consultants, certain service providers. It may also include the personal data of other people which pupils acquire through schoolwork tasks or while at school e.g., survey results, class Christmas card lists, and pupils will have some responsibilities in line with their capacity to understand and follow rules.

The following definitions explain a little more about our approach to personal data:

'Data processors' are third party organisations which process data on our behalf. They make no decisions about how and why they do that; they just do what we ask them to within the terms of our contract.

'Data subjects' are the people about whom we hold data, and they fall into several general "categories of person", for example, our workforce and their next of kin; pupils, their next of kin, and other professionals involved with them; our contractors (cleaners, caterers, health & safety, and other service providers); agency and other partner organisation workers (supply or peripatetic teachers, educational psychologists).

'Personal data' is any manually or digitally recorded information relating to a living person (a data subject) which identifies them e.g., a name, an email address, an identification number, location data, an image, an IP address, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person and may include facts or opinions about them. Some of this category of personal data will require enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g., a locked filing cabinet. This will be determined on the basis of a risk assessment of the harm that failing to secure the data might cause e.g., bank details due to the risk of potential fraud, contact information due to potential harassment etc.

'Sensitive personal data' or **'special category data'** includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical, and religious opinions/beliefs, trade union membership, and details of criminal convictions or allegations. This category of personal data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls.

'Pseudonymised personal or sensitive personal data' is information that has been de-personalised but key-coded and it can fall within the scope of the UK GDPR and this policy depending on how difficult it is to attribute the pseudonym to a particular individual.

'Supervisory Authority' is the body that regulates compliance with the GDPR and in the UK this is the ICO.

'third country' is the designation given to a country where there is no privacy and security of data equivalence agreement and transfers of personal data are restricted unless the data is specially protected, or an exception applies. The UK is a 'third country' to states in the EU GDPR zone (the EU member states plus Norway, Liechtenstein and Iceland) so, The exceptions that apply to the UK are the adequacy decision on transfers under EU GDPR and the adequacy decision on transfers under the Law Enforcement Directive on data transfers between the EU and UK. A 'third country' to the UK, is any state or country worldwide which is not a part of the UK and to which the UK under UK GDPR restricts transfers of personal data unless the personal data is specially protected, or an exception applies. The exceptions that apply to some of these 'third countries' are limited and described in the adequacy decisions the UK has made (see Section 10.5 for more information).

We will make anyone with whom we share the personal data of our data subjects aware of our relevant policy, procedures, and expectations at the outset of sharing.

Any breach of this policy, or of the Regulation itself must be reported to our Data Protection Officer and may need to be reported to the ICO as the Supervising Authority for the United Kingdom. The breach could be unlawful and result in legal action or prosecution and regardless of any legal repercussions it may also be actionable under our disciplinary procedures.

This policy will be updated as necessary to reflect improving practice in data management, security, and control and to ensure compliance with any changes to relevant legislation.

Associated policies or documents include:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Online Safety Policy and procedures
- Freedom of Information Publication Scheme
- Health and Safety Policy and procedures
- Procedures for Using Pupils' Images
- Behaviour Policy and procedures
- Staff Code of Conduct

2. Roles and responsibilities

Our responsibilities as a data controller include:

- Analysing and documenting the types of personal data we hold and their uses.
- Identifying our lawful basis for processing personal data.
- Having procedures which support the rights of the individual.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect, report, and investigate personal data breaches.
- Storing data in safe and secure ways.
- Assessing risks to individual rights and freedoms should data be compromised.

Staff responsibilities include:

- Understanding their data protection obligations in line with their training and professional duties, and with our relevant Policies and procedures e.g., the Online Safety Policy when remote working etc.
- Checking that their data processing activities comply with our policies and are justified.
- Not using data in any unlawful way.
- Storing data carefully and correctly to avoid breaches of data protection.
- Raising concerns, notifying breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations without delay.

The Data Protection Officer's responsibilities include:

- Keeping governors/trustees updated about data protection responsibilities, risks, and issues.
- Reviewing the data protection policy, associated policies, and all relevant procedures regularly.
- Arranging data protection training and advice for all staff and others included in this policy.
- Advising on direct marketing issues such as compliance with the law and our policy; how we deal with queries from target audiences or media outlets; and the wording of data protection statements attached to emails and other marketing copy.
- Answering questions on data protection from staff, governors/trustees, and other stakeholders.
- Responding to individuals such as parents, pupils, and employees who want information.
- Checking on and approving of any third parties that handle our data and any contracts or agreements regarding data processing.

The Information Technology Manager's responsibilities include:

- Ensuring all systems, services, software, and equipment meet acceptable security standards and can be appropriately filtered and monitored.
- Checking security hardware and software regularly to ensure it is functioning properly and securely.
- Researching relevant third-party services (cloud services, data shredding etc.) that we are considering using.

3. Data protection principles

We understand that as a data controller we are responsible for, and need to be able to demonstrate that we comply with the principles set out in Article 5 of the GDPR which requires that:

a) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

We aim to achieve this through carefully considering why we need data before we ask people for it; by publishing our Privacy Notices, implementing them and reminding people about what the notices says when we ask for data; and by educating our workforce on what they mean for their day-to-day practice.

b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

By keeping our Privacy Notices updated, implementing them, and educating our workforce about what we have and have not agreed to use data for (also in line with requirement a) above), we can ensure we meet this obligation to restrict our processing of personal data. The law does allow us to further

process data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notice.

c) Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

We will not seek to collect or process personal data which is not strictly necessary for the reasons we asked to be given it. We keep this in mind when we draft data requests and when irrelevant information is provided, we take all reasonable steps to return or erase it.

d) Personal data shall be accurate and, where necessary, kept up to date.

We review and update personal data on a regular basis. It is the responsibility of individuals providing personal data to ensure it is accurate. Individuals should notify us by any reasonable means, but preferably in writing, if their personal data needs to be updated e.g., a change of name or contact details. We will take every reasonable step to ensure that inaccurate personal data (after considering the reasons it is being processed), is erased or rectified without delay, for example, some records are historical and should not be changed.

e) Personal data shall be kept for no longer than is necessary.

We will not retain personal data in a form which allows people to be identified for longer than is necessary to use it for the reasons we asked for it. We employ organisational and technical security measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals, as well as follow strict information transfer guidelines when we need to move data e.g., when a pupil leaves to attend another school. We hold regular reviews of the data we retain and destroy and archive in line with guidance from Cumberland Local Authority - Retention and Disposal Schedule xlsx (live.com) and Retention Schedule quick user guide v.1.0 (cumbria.gov.uk) and the IRMS Schools Toolkit - Information and Records Management Society

The law does allow us to retain personal data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notices.

f) Personal data shall be processed in a manner that ensures appropriate security of it.

We understand that our organisational and technical measures to protect data must include protection against unauthorised or unlawful processing and against accidental loss, destruction or damage in the UK, European Union or anywhere else in the world.

We make staff and volunteers aware of their data protection responsibilities and that their duty to preserve confidentiality extends to anywhere that they process the data of our data subjects e.g., at home, on trips etc. and beyond their time of employment with us. See Section 10.2 for more information about the organisational and technological measures we employ to achieve this.

The first principle of data protection is **fair, lawful, and transparent processing**, and is the foundation on which everything else is built. We seek to meet the "fair" and "transparent" aspects through our Privacy Notices, and we work hard to ensure that all of the personal data we process meets a condition for lawful processing so that we have a lawful basis to carry it out.

3.1 Conditions for the lawful processing of personal data

To process a piece of personal data we must satisfy at least one condition for the lawful processing of personal data from Article 6 of the GDPR set out in the table overleaf.

6(1)(a)	Consent of the data subject.
6(1)(b)	Necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
6(1)(c)	Necessary for compliance with a legal obligation.
6(1)(d)	Necessary to protect the vital interests (life) of a data subject or another person.

6(1)(e)	Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6(1)(f)	Necessary for legitimate interests of the controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject (not available to processing carried out by public authorities in the performance of their tasks).

We rely on different conditions for the lawful processing of personal data for different things.

To process the personal data of our workforce and volunteers we generally rely on 6(1)(b) i.e., to employ them and provide training, uniform, pay etc. Some pieces of data are processed for other reasons. For example, we use their national insurance number for tax purposes relying on 6(1)(c); we hold their next of kin data relying on 6(1)(d); and we use their image relying on 6(1)(f) regarding surveillance cameras and staff/visitor ID badges and sometimes 6(1)(a) e.g., any publishing that is not necessary.

To process the personal data of our pupils we generally rely on 6(1)(e) i.e., to educate them. Some pieces of data are processed for other reasons. For example, we publish their SATs results relying on 6(1)(c) because the law requires us to; we hold their next of kin data relying on 6(1)(d); and we use their image mostly relying on 6(1)(f) but sometimes relying on 6(1)(a) e.g., publishing.

We rely on different conditions to process different pieces of the personal data of families e.g., 6(1)(b) for their financial details to provide meals, photographs etc.; and 6(1)(d) for their contact details in case their child is ill. We use the same criteria to process the personal data of other individuals such as contractors or Local Authority workers etc. where it applies and most often using 6(2)(b) to work together.

3.2 Conditions for the lawful processing of special categories of data

To process a piece of sensitive personal data we must satisfy at least one condition for the lawful processing of special categories of data from Article 9 of the GDPR set out the table below **as well as** one condition from the previous table.

9(2)(a)	Explicit consent of data subject, unless prohibited by EU/National law.
9(2)(b)	Necessary to meet obligations under employment, social security or social protection law, or a collective agreement.
9(2)(c)	Necessary to protect the vital interests (life) of a data subject or another individual where the data subject is physically or legally incapable of consenting.
9(2)(d)	Processing by a not-for-profit body with political, philosophical, religious or trade union aims if it relates only to members/former members (or those in regular contact for those purposes) & there is no disclosure to third parties without consent.
9(2)(e)	Processing relates to personal data already made public by the data subject.
9(2)(f)	For the establishment, exercise or defence of legal claims or court judicial capacity.
9(2)(g)	Substantial public interest under EU/National law proportionate to the aim pursued and which contains appropriate safeguards.
9(2)(h)	For preventative or occupational medicine; assessing work capacity of an employee, medical diagnosis, providing health & social care or treatment or management of healthcare services under EU/National law or contract with a health professional.
9(2)(i)	For public health e.g., protecting against serious cross-border threats to health or ensuring high standards of healthcare & medicinal products or medical devices.

We rely on different conditions for the lawful processing of sensitive personal data for different things.

To process the sensitive personal data of our workforce and volunteers we rely on 9(2)(b) to check their criminal history before employing them; 9(2)(h) to use their health information to protect them at work; 9(2)(a) to share their health information with support services; 9(2)(i) to report on their health to the UK

Health Security Agency (UKHSA), local Health Protection Team (HPT) or the Health & Safety Executive (HSE) as required; and 9(2)(f) to retain accident and ill-health information in case of a claim for compensation.

To process the sensitive personal data of our pupils we rely on 9(2)(b) in respect of child protection and multi-agency safeguarding work; 9(2)(b) or 9(2)(h) to use their health information to protect them at school; 9(2)(i) to report on their health to UKHSA, local HPTs, or the HSE as required; and 9(2)(f) to retain accident and ill-health information in case of a claim for compensation.

We apply the same criteria to processing the sensitive personal data of families and other individuals such as contractors or Local Authority workers etc. where it applies.

3.3 Deciding which condition to rely on

More than one lawful basis may apply, but we only need **one** basis for each piece of data, and we will rely on what best fits the purpose, not what is easiest. When carrying out a new task or an existing task in a new way, staff should consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request, and have we factored in how to do this?

3.4 Privacy Notices

Our Privacy Notices are an important and necessary way of being transparent and telling governors/ trustees, parents, pupils, staff, contractors, and visitors what we are doing with their information. To comply with the law, it will include:

- Our identity and contact details as the data controller and those of our DPO.
- The purpose of the processing and the lawful basis or bases we are relying on.
- Our, or a third party's legitimate interests in having it.
- The categories of personal data we process.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to UK Government determined "third countries" and the safeguards.
- Retention periods or the criteria used to determine them.
- The existence of each of the data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with the ICO.
- The sources of personal data and whether they are publicly accessible.
- Whether providing personal data is statutory or contractual and the possible consequences of failing to provide it.
- The existence of any automated decision making, including profiling; how decisions are made, the significance and the consequences.

See the Contents Page for links to our privacy notices relevant to pupils, our workforce and volunteers, our governors/trustees, and visitors. They are also made available on our website, on noticeboards, and in communications with parents and staff etc.

4. Individuals' rights and how we protect them

We recognise that all data subjects have "qualified rights", so they are not absolute rights in all circumstances. They are qualified by the rights of other individuals and the legal rights of the data controller or processor to conduct their lawful business.

4.1 The right to be informed about the collection and use of their personal data

Our Privacy Notices seek to provide transparency about our collection of personal data; they are published on our website, pinned to noticeboards, and freely available on request from our office; we draw people's attention to what they say when we collect data from them; and we regularly review and update the Notices when necessary, particularly if we have changed what we use the data for and before we start using it for the new reason.

4.2 The right of access to their personal data and relevant supplementary information

This includes:

- confirmation that their data is being processed.
- access to their personal data; and
- other supplementary information which largely corresponds to the information we must provide in our Privacy Notices.

Any of our data subjects (or their chosen representative or a person with parental responsibility for them) can make a Subject Access Request (SAR). Please see Section 5 for our procedure on handling SARs.

4.3 The right to rectification if the information held is inaccurate or incomplete

Every individual has a responsibility under UK GDPR to provide accurate data. There is no legal definition of accuracy, but we generally understand it to mean that personal data is inaccurate if it is incorrect or misleading on matters of fact.

The right to rectification will depend on why we asked for the personal data. For example: a person's name should **not** be changed to their new married name on the Single Central Record (SCR) because the SCR is a record of information correct at the time of recruitment and vetting. A note should be added to ensure the SCR record can be matched to the correct living person in case of a vetting query using the married name in future, but the record itself should not be changed.

When we receive a request to change the data we hold, we will take reasonable steps to check that the data is accurate and to rectify it if necessary. This means that the more important it is that the data is accurate, the more effort we will make to correct it. We will take into account arguments and evidence provided by the data subject and anything we have already tried to do to ensure the data is accurate.

We can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether it is repetitive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one mon**th. We do not have to comply with the request until we have received the fee.

As a matter of good practice, we will restrict the processing of the personal data in question while we are verifying its accuracy regardless of whether the data subject asked us to as is their right (see Section 4.5).

When we have decided whether the data is accurate or not and whether we will change it or not, we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of the request and our response similar to the way we handle SARs e.g., date of receipt, the data subject's name, the name, and address of requester *(if different)*, the rectification requested, our decision, and the date we communicated the decision.

4.4 The right to erasure of personal data

Under Article 17 of the GDPR individuals have a new right to have their personal data erased. This is also known as the "right to be forgotten". There are no rules about how a request should be made e.g., verbally, in writing etc. so all staff are trained to recognise someone trying to exercise this right. The right is not absolute and only applies if:

- the personal data is no longer necessary for the reason we originally collected or processed it.

- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent.
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue e.g., our use of surveillance cameras is an overriding legitimate interest for us in order to prevent and detect crime, not to satisfy our public duty to provide education.
- we are processing the personal data for direct marketing purposes and the individual objects.
- we have processed the personal data unlawfully i.e., in breach of the lawfulness requirement of the 1st principle.
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer online "information society services" remotely online directly to a child under the age of 13 e.g., an app, game, social media platform etc. Any such services we currently provide, or broker are necessary for education purposes (or are exempt because they are counselling services) so the right to erasure may not apply, but we are aware of our obligations and will act accordingly. We also work hard to appropriately control children's access to the social media platforms we use to communicate with our community.

We have to give special consideration to any request for erasure if the processing of the data is solely based on consent given by a child, especially any processing of their personal data (usually images) on the internet. This is still the case when the data subject is no longer a child because a child may not have been fully aware of the risks involved in the processing at the time of consent. In some circumstances we might need to give more weight to a request for erasure from a child if their parent has already consented to the use of their data e.g., removing pictures from our school website when a parent has consented but the child whose images they are objects. We will need to do this if we are confident that the child understands their rights and the effects on them of their request. For more information about how we decide whether a child understands please see Section 5 on Subject Access Requests.

Unless it is impossible or disproportionate, we have to tell other organisations about erased data if:

- the personal data we erased has been disclosed by us to others; or
- the personal data has been made public in an online environment (for example on social media, forums, or websites).

If we are asked, we should also tell the individual about the other organisations we gave their data to.

The right to erasure does **not** apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information.
- to comply with a legal obligation.
- for the performance of a task carried out in the public interest or in the exercise of official authority.
- for archiving purposes in the public interest, scientific research, historical research, or statistical purposes where erasure is likely to make achievement of that processing impossible or disproportionately difficult; or
- for the establishment, exercise, or defence of legal claims.

There are also two circumstances when the right to erasure does **not** apply to special category data:

- if the processing is necessary for public health purposes in the public interest; or
- if the processing is necessary for the purposes of preventative or occupational medicine.

When we receive a request to erase data, we will take reasonable steps to check the identity of the requester and that they have the right to make the request before considering it.

We can refuse to comply with a request when an exemption applies, or when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one month**. We do not have to comply with the request until we have received the fee.

When we have decided whether we can erase the data we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of the request and our response similar to the way we handle SARs e.g., date and manner of request (verbally to class teacher, a note handed to reception etc.), the data subject's name, the name and address of requester *(if different)*, the erasure requested, our decision, and the date we communicated the decision.

4.5 The right to restrict the processing of personal data

Under Article 18 of the GDPR individuals have the right to limit the way we use their data if they have a particular reason for wanting to, and this is an alternative to erasing it. They may have issues with the content of the information or how we have processed it. In most cases we will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time. The right is not absolute and only applies if:

- the individual contests the accuracy of their personal data and we are verifying it.
- the data has been unlawfully processed i.e., in breach of the 1st principle, and the individual doesn't want it erased.
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

We use the most appropriate method applicable at the time to restrict processing including:

- temporarily moving the data to another processing system.
- making the data unavailable to users; or
- temporarily removing published data from a website.

While a restriction is in place, we will not do anything with data except store it unless:

- we have the individual's consent.
- it is for the establishment, exercise, or defence of legal claims.
- it is for the protection of the rights of another person; or
- it is for reasons of important public interest.

If we have disclosed the restricted data to another organisation, we will tell them about the restriction in the same way as if it were inaccurate data unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

We can lift the restriction when we have decided that the issues are resolved i.e., the data is accurate, or our legitimate grounds override the individuals', and we will inform the individual and include our reasons before we lift it. We will also tell them about their right to make a complaint to the ICO.

We can refuse to comply with a request when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay. We do not have to comply with the request until we have received the fee.

4.6 The right to data portability

The right to data portability only applies when all 3 of the following conditions are met:

- the individual has provided the personal data.
- the processing is based on the individual's consent or for performance of a contract; **and**
- processing is carried out by automated means.

We do not currently hold any qualifying data, but we are aware of our legal obligations and will follow ICO guidance, reviewing our procedures if we automate any processing.

4.7 The right to object to processing

Individuals must have an objection on "grounds relating to his or her particular situation" and we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or
- the processing is for the establishment, exercise, or defence of legal claims.

We will:

- inform individuals of their right to object "at the point of first communication" and in our privacy notices, explicitly bringing the right to their attention clearly and separately from any other information.
- stop processing personal data for *direct marketing purposes* as soon as we receive an objection because there are no exemptions or grounds to refuse; and
- deal with an objection to processing for *direct marketing* at any time and free of charge.

An individual can object to processing for research purposes on "grounds relating to his or her particular situation" unless processing is necessary for the performance of a public interest task.

We carry out some processing of personal data securely in encrypted online systems e.g., our visits approval system, responding to DfE data demands online, and any individual can object to our online processing by contacting us at admin@stherberts.cumbria.sch.uk.

4.8 The right to object to automated decision making and profiling

We do not currently use any data systems that make automatic decisions about people without any human involvement. We are aware of our legal obligations and will follow ICO guidance, reviewing our policy and procedures if we fully automate any decision-making.

5. Subject Access Requests (SARs)

Every individual who is our data subject has the right to access their personal data so that they are aware of and can verify the lawfulness of the processing, including children of any age who understand what they are requesting. These rights do not automatically override the rights of any other individual who might be identified by our response to a request, so we will make a decision on what information to disclose by balancing the data subject's right of access against any other individuals' rights in respect of their own personal data. We will use the latest ICO guidance on SARs to help us make decisions.

The data subject or the person acting on their behalf must make a SAR in writing, and we provide a form to help people do this (see Contents Page for link). There is no requirement to use our form, but it can speed up the process by helping the people making requests to provide us with the kind of information we need to comply. We will also make any reasonable adjustment for disabled people who may be unable to make their SAR or receive information in writing e.g., accepting a verbal request, providing a braille response etc. Relevant staff are trained to recognise a SAR even when it does not include the words "subject access", or refer to the applicable legislation, including where the wrong legislation is quoted i.e., often the Freedom of Information Act.

When we receive a SAR, it will be entered in the Subject Access Request logbook, including the date of receipt, the data subject's name, the name, and address of requester *(if different)*, the type of data requested (e.g., pupil record, personnel record), whether there is enough information to respond appropriately (and the immediate action taken to seek more if not), and the expected date for providing the information.

We aim to provide information without delay and at the latest **within one month** of receipt of the request. For example: if we receive a SAR on the 10th of the month we will respond by the 10th of the following month. We will seek to extend this response period by up to the two further months which the law allows where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

SARs made by pupils will be processed in the same way as any other SAR and the information will be provided to the child regardless of their age unless it is clear that they do not understand their rights. If we are sure that the pupil **does not** understand the SAR and their rights, we will refer the matter to parents, comply if they agree, and provide the information to parents.

SARs made by people on behalf of children they hold parental responsibility for will be processed in the same way as any other SAR while recognising that they do not own the data they are requesting. If we are confident that the pupil whose data it is **does** understand the SAR and their rights, then we will respond to the child rather than the parent, even where the parent was the one who made the request.

In making our decision we will take the following, amongst other things, into account:

- the child's level of maturity and their ability to make decisions like this.
- the nature of the personal data.
- any court orders relating to parental access or responsibility that may apply.
- any duty of confidence owed to the child or young person (including information about any counselling or other service being offered directly to the child).
- any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment).
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

If the information requested by a parent in a SAR relates to the 'educational record' of a pupil, in accordance with *'The Education (Pupil Information) (England) Regulations 2005'*, we will make a pupil's educational record available for inspection by the parent, free of charge, **within fifteen school days** of receipt of the parent's written request for access. This cannot include any information that we could not lawfully disclose to the pupil themselves. If parents request a copy to keep, we can charge the administrative costs of supplying one.

If the information requested in a SAR does **not** relate to the 'educational record' of a pupil, we will provide a copy of the information free of charge **unless** the request is manifestly unfounded or excessive, particularly if it is repetitive. This fee may vary and will be based only on the administrative cost of providing the information. We will use ICO guidance and our own information management records to make decisions about this.

We must verify the identity of the person making the request, using "reasonable means". If the person making the request is not the data subject, we must also verify their right to make such requests on behalf of the data subject e.g., their authority to act or their parental responsibility for a child. In cases where a child is competent to make their own request, information will be provided to the child and not to the parent. We will use ICO guidance and our knowledge of the capability of our pupils as described above to make decisions about this.

If the request is made electronically, we will provide the information in a commonly used electronic format.

If we are asked for a large quantity of information about an individual, we can ask the individual to be more specific about the information they want. This is not because we are exempt from providing large amounts of data, this is so we can consider whether the request is manifestly unfounded or excessive.

If we are asked for information that a data processor, we work with holds on our behalf, we will ask our data processor to provide it to us so that we can comply with the SAR. This is because we are the data controller, and it is our responsibility. We have written contracts in place with all of our data processors to help us do this.

A Subject Access Request should be made in writing to Mr Michael Craig, Headteacher.

6. Data protection and privacy by design

Data protection and privacy by design is an approach to projects and tasks that promotes privacy and data protection compliance from the start and is a clear legal requirement of us. This is not just about the

strategic decisions we make building new IT systems for storing or accessing personal data and developing policy or strategies that have privacy implications. It is also about collecting or sharing data in a new way or using data for new purposes.

Our aim is to minimise privacy risks and build trust so all staff will have a central role to play in keeping what we do compliant. When handling data in a different way staff are trained to first consider the impact of what they are doing and how they are doing it in relation to data protection and privacy, with the ten questions in Section 3.3 playing an important part in the process. This could be as simple as ensuring consent forms containing sensitive personal data are not carried in a clear folder on a trip, or as complex as thoroughly vetting an overseas data transfer service when a pupil leaves us to attend a school outside the European Economic Area (EEA).

We use the ICO guidance on Data Protection Impact Assessments (DPIAs) as an integral part of our approach to data protection and privacy by design. We also consult our DPO at the outset of any new data project.

6.1 Data Protection Impact Assessments (DPIAs)

We understand that we have a legal obligation to do a Data Protection Impact Assessment (DPIA) before carrying out processing likely to result in a high risk to individuals' interests. We will use the ICO template to help us get this right. When it involves surveillance cameras, we will use the government guidance and template, Data protection impact assessments for surveillance cameras. If our DPIA identifies a high risk which we cannot mitigate, we must consult the ICO before proceeding.

A DPIA is a process to systematically analyse our processing and help us identify and minimise data protection risks. It is meant to:

- describe the processing and our purposes.
- assess the necessity and proportionality of what we are planning.
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk but should help to minimise risks and consider whether or not they are justified. We will need to do a DPIA if we plan to:

- use new technologies.
- use profiling or special category data to decide on access to services.
- profile individuals on a large scale.
- process biometric or genetic data.
- match data or combine datasets from different sources.
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing').
- track individuals' location or behaviour.
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

All staff have a responsibility to identify when their activities around data imply the need for a DPIA. This could be doing an entirely new task with data, or it could be changing the way a well-established task is being done. Any need for a DPIA should be reported to Mr Michael Craig, Headteacher.

7. Training & Awareness

During their induction, all staff and volunteers will receive suitable training in their responsibilities for data protection in their work or volunteering, and the relevant procedures. This will be supplemented with staff briefings, inset training, and other methods of updating staff and volunteers as necessary e.g., briefing emails, notices etc.

This policy is available to all staff electronically on the staff network (S:/Policies) and it is available publicly on the school website. This policy will be updated regularly in line with changes in practice or clarifications required after applying it to resolve data protection issues.

Anyone can seek general data handling guidance from the ICO on their website https://ico.org.uk.

Day-to-day support and guidance for staff is available from Michael Craig, Head teacher and/or Reverend Charles Hope, DPO. Any other category of person wanting help with a data protection issue e.g. contractors, parents etc. can also contact the school office or are free to contact our DPO using the published contact details.

8. Publication of Information

At times we publish information which includes personal data, for example:

- our internal telephone and email directory,
- event information,
- staff information such as who's who on our website,
- lists of students in a team.

Some things we publish can be subject to an individual's consent and we will seek it as required and consider all reasonable requests to correct, erase, or restrict data processing in line with our legal obligations.

9. Managing Consent

We only need one lawful reason to process personal and special category data and the law provides us with 6 reasons to choose from for personal data (see Section 3.1) and 9 reasons for sensitive personal data (see Section 3.2). This means it is extremely rare for us to have to rely solely on consent as our *only* lawful basis for processing.

When we do need consent and we ask for it, we will include the following information in our request:

- the name of our school.
- the name of any third-party controllers who will rely on the consent.
- why we want the data.
- what we will do with it; and
- that individuals can withdraw consent at any time.

People will be asked to actively indicate their consent in words and if there are different options, these will be made clear e.g., consent for a child to participate in an event being clearly separate from any consent to use images of them taken at the event (if no blanket/lasting images consent is already held).

There is no set time limit for consent. How long it lasts depends on the context and what we have told people in our Privacy Notices or other communications. We review and refresh consents as appropriate.

Genuine consent should put individuals in control, build trust and engagement, and enhance our reputation so, when we do rely on it, we need to keep a record that helps show it was freely given e.g., who consented, when, how, and what they were told.

9.1 Consent to use personal data including images and voice recordings

We do not need parental consent to process any personal data including image or voice recordings for the purposes of education e.g. photographs or video of a child demonstrating how they meet a learning outcome. Using names, image, and voice recordings of children in their work and in displays inside school, is a fundamental part of their education, personal development and how we celebrate them. This does not affect the statutory rights of individuals as set out in Section 4. Anyone can raise any concern with any member of staff about our use of their or their child's data at any time and we are obliged to ensure their rights are upheld where we have no lawful reason to refuse.

We *may* need parental consent to use personal data including image and voice recordings for other reasons such as marketing or self-promotion in publications and on websites or social media platforms directly

managed by us or, with our permission, by others associated with us which may include pictures of living people that have been drawn by children.

Images that might cause embarrassment or distress will not be used nor will image or voice recordings of children be associated with materials or issues that are considered sensitive. Anyone with parental responsibility for a child can ask to see any images that we hold of them at any time.

There is no legally binding age of consent in the UK with regard to the use of an individual's own data, including their image or voice, except on organisations providing an Information Society Service (ISS) directly to a child online and solely on the basis of their consent (which is aged 13). We do not currently offer any ISS and have no plans to. This means that any child of any age can assert their data rights or consent to the use of their data under the law, providing we are sure that they understand their rights and the implications of their consent. For more information about how we make decisions about a child's competence to consent or withdraw consent that their parents have previously provided, please see Section 5.

Photography, audio recording or filming will only take place at school or school events with the permission of the Head teacher/ manager, and under appropriate supervision.

Regardless of who is publishing data, and that includes us, our policy is that children will only be named if there is a particular reason to do so e.g., they have won a prize, and no other personal details will be published or given out. If names will, or might, be published e.g., in a newspaper article, we will check that parents understand the potential implications and consent to the use of names at that time and before the publishing happens. The news media will often require a child's full name before they will publish an image and our policy is to resist this wherever possible and if we fail, we will take steps to ensure that parents are aware that all of the details will be available in local or national newspapers and worldwide online.

We allow parents, carers, and other invited visitors to take images of children at school functions, but we reserve the right to enforce special restrictions on a case-by-case basis. They are required to bear in mind that they may capture other people's children and must ensure images are appropriate.

We explain the rules in writing in event information beforehand, at events with appropriate signage when necessary and an announcement at the start, and we will take reasonable steps to enforce it.

Rules may vary between events but will always include:

- Where photography and filming is permitted or not permitted.
- That photography and filming is permitted for strictly personal and private use only, that everyone has a responsibility to ensure images they keep, and share, are appropriate, and that they should not be shared on social media without the express permission of everyone in them (and/or their parents or carers).
- That those who want to take pictures or film must not disturb other people's view or enjoyment.
- A reminder about our Behaviour Policy and Online Safety Policy which says that no child or adult associated with us in any way should ever upload or post online any content (pictures, audio, video, or text) that could upset, offend, or threaten the safety of any member of our community or bring us into disrepute.

Our policy on requesting consent is to ask once when a child starts their career with us for separate general consents to use image and/or voice recordings:

a) By publishing them on our website or in other print or online media which we directly control, or
b) By allowing carefully selected third party organisations such as local media outlets to publish them.

We use a form to seek blanket/lasting consent (see Contents Page for link) and we remind parents and children regularly that they can change or withdraw their consent at any time.

When a child understands their right of consent and its full effects and there are no reasons why their name, image or voice must be protected, we can prioritise the consent of a child over parental consent where they are different. We are more likely to decide not to use images etc. when a child objects and their parent does not than vice versa, but our overriding priority will always be to act in the child's best interests.

Staff are expected to make themselves aware of any guidance we use from the ICO, our local authority, Local Safeguarding Children Partnership, or governors and our competent advisors e.g., KAHSC Safety Series: G21 The Use of Images Working with Children to apply the principles in all use of image and voice recordings.

9.2 Consent for the use of generative artificial intelligence (intellectual property)

Most generative artificial intelligence (AI) tools will use the inputs submitted by users to further train and refine their models.

However, pupils own the intellectual property (IP) rights to original content they create. Original content is likely to include anything that shows working out or is beyond answers to multiple choice questions. Intellectual property can only be used to train AI if there is consent from the rights holder or an exemption to copyright applies.

Some tools allow users to opt out of inputs being used to train the models.

Staff training includes that, as a school, we must not allow or cause pupils' original work (content) to be used to train generative AI models unless we hold appropriate consent or exemption to copyright. Without this, staff are responsible for ensuring that, every time they input pupil's original work, they have opted out of the inputs being used to train the AI models.

Most generative AI tools have terms of service that include a minimum age of 13 years for users but also requires all users aged 13-17 to have the consent of their parent or legal guardian to use them.

This means that pupils must not use these tools at all and that staff must not input pupils' original work into these tools, unless they opt out of allowing its use for training the AI models, if they don't have evidence that parents have consented to this use of their child's intellectual property. Consent to opt in to sharing pupils' original work to train AI models must be an additional question separate from whether parents consent to their child's original work being input into generative AI tools.

Currently, this school supports limited analytical, administrative and educational use of Open AI services such as ChatGPT & DALL-E and Google AI to reduce staff workloads and enhance learning.

Parents of pupils whose original content will be input into a generative AI tool are sent links to the tool terms of service beforehand, EU terms of use | OpenAI and Google Terms of Service – Privacy & Terms – Google]. We ask them to read these Terms with their child to ensure they understand and agree to them. Parents who receive this information are expected to respond confirming whether they consent to original work by their child aged 12 or under being input into a generative AI tool and additionally whether they consent to their child's original work being used to train AI models.

We will take steps to explain to all pupils when relevant, in age/developmental stage appropriate ways, the function and risks of using their original content (and potentially their personal data if they used it to make their content) to contribute to global machine learning. We may not explicitly ask pupils for their consent on issues of intellectual property but they will be taught about online safety and that their opinion of what will happen to their original work or to their personal data matters. An agreement to use their intellectual property from anyone aged 13-17 can *never* override a parent's refusal to consent, but if a parent agrees and their child doesn't, we might decide *not* to use their child's original work. This is because we may need to be sensitive to issues around low self-esteem and anxiety or other mental health issues that can become worse when a pupil feels they lack control over decisions that they feel impact them negatively.

Exemptions to copyright are limited, and if there are any concerns about whether we are acting within the law, current DfE advice suggests we may wish to seek legal advice. This means that all questions or concerns about our use of generative AI should be treated seriously and directed to the Headteacher.

9.3 Data sharing during a public health emergency: consent and data retention

In line with our statutory duties, we require anyone who comes into close contact with our pupils. staff, buildings, or equipment (including our staff and pupils) to share with us necessary personal data to give to an organisation authorised by a relevant public health authority so they can take action to protect public health. We do not need consent for this and in a public health emergency this is no different to our normal

practice when we are required to report that staff or pupils have contracted a notifiable disease like meningitis or measles, or if we have a food poisoning incident on our premises.

10. Data Security and Integrity

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be: "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The security measures we put in place seek to ensure that the data:

- can be accessed, altered, disclosed, or deleted only by those we have authorised to do so and that those people only act within the scope of the authority we give them.
- is accurate and complete in relation to why we are processing it; and
- remains accessible and usable, i.e., if personal data is accidentally lost, altered, or destroyed, we should be able to recover it and prevent any damage or distress to individuals.

All staff and any others who process the personal data of our data subjects are expected to work to the same principles we do at all times.

10.1 Classification of data

We carry out regular data audits to identify data that we control and the risks to every kind of processing we do to that data, and we keep a record to help us deal with any issues or requests. As part of this systematic approach, we operate 3 levels of data classification to ensure the appropriate security measures can be taken to keep the data safe:

- **Public:** Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain e.g., the information the DfE publishes about our governors/ trustees on the Get Information About Schools public database online.
- **Confidential:** Information that, if disclosed inappropriately, may result in minor reputational or financial damage to the school or may result in a minor privacy breach for an individual. Information that should only be available to sub-groups of school staff who need the information to carry out their roles.
- **Sensitive:** Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.

The appropriate marking of data as to its classification is an operational decision on a case-by-case basis. Most of our data held in electronic databases is classified automatically by the information management systems that hold it. Information that is transferred e.g., emailed, posted, moved to an archive etc. must be appropriate classified and marked to ensure it will be treated properly.

Appendix A sets out some of our specific data security expectations at each different level of data classification and we share it with staff and others who have legal obligation to us when they process data that we control.

All data classifications are reviewed at the point of entry into our archive. All archived data is appropriately labelled with:

- the final data classification.
- any specific restrictions i.e., not to be released to named parent under court order.
- how the data is to be destroyed e.g., incineration, cross-cut shredding, shredding, or electronic data scrubbing/shredding.
- when the data is to be destroyed.

Staff responsible for archiving are trained to assess and manage any increasing risks that can arise as data about one person is aggregated.

10.2 Organisational and technical security measures

The main organisational and technical measures we employ include:

- Appropriate physical security measures for the site, buildings, restricted areas, and restricted storage containers including locks, restricted access codes and alarms.
- Appropriate physical access and security procedures including limiting access to areas or stores to certain key holders, and procedures to welcome visitors aimed at preventing unauthorised access e.g., visitors' badges, signing in/out, whether a visitor can only access certain areas while accompanied etc.
- Ensuring unauthorised personnel cannot see documents or screens which might display personal data e.g., open registers and visitor's books, emails, surveillance camera monitors.
- Suitable contracts of employment or technology access agreements for pupils, visitors and others aimed at ensuring the proper use of personal data and maintenance of confidentiality.
- Appropriate storage arrangements that avoid physical risks (flood, fire etc.), loss (lost devices, accidental destruction etc.) or electronic degradation (corruption caused by electricity or magnetism, new software unable to read files created using old software etc.).
- Appropriate technological or procedural security measures including:
    - The installation of appropriate security software (including for virus and malware checking) on all devices used to process personal data, instructions on how to use it properly, and the requirement on all data users to adequately secure devices i.e., carrying portable devices securely and activating an encrypted screen lock when leaving a device unattended even for a minute.
    - Restricting access to school devices containing personal data to employees and specially authorised volunteers, visitors, or service providers. Staff using a work device off-site must take steps to secure their work device from use by anyone else including family.
    - Enforcing our strict protocol on the use of personal devices to process personal data obtained at work, including a requirement for secure remote access to school systems (please see Online Safety Policy/ Acceptable Use of IT Policy/Agreement/ Staff Code of Conduct);
    - Restricting the number of people who can access certain data by limiting online logins, protecting parts of our network to hide them from unauthorised users, and by having procedures in place to designate authorised users and give only them the proper access;
    - Enforcing our strict password protocol for access to any personal data whether it is online, on a device, or being transferred somewhere e.g., email. All staff who use Password Managers are required to apply the best practice guidance blog from the National Cyber Security Centre (NCSC).
    - Having appropriate data recovery arrangements in place to avoid accidental loss of data or password sharing i.e., so when someone is unavailable to provide access to data, with the proper authorisation their access can be reset and the data still obtained in their absence.
    - Appropriate marking or designating of data as private or confidential or sensitive to ensure it is treated accordingly e.g., not printed to a publicly accessible printer.
    - Adherence to strict controls on the transfer of data i.e., only as authorised and agreed via encrypted email or portable device, secure websites, password protected files, properly addressed and if necessary fully tracked postal packages, delivery by hand etc.
    - Secure methods of disposal for both paper and electronic data shredding.
    - Clear policies and procedures for the appropriate archiving and automatic backing up of necessary data including off-site e.g., essential data identified in the Emergency Preparedness Plan to ensure business continuity.
    - Clear and binding contracts with our data processors such as our health & safety provider and people who we jointly control data with such as the outdoor adventure centres we go on residential trips to.

All enquiries about the policies and procedures that should be followed and how data should be protected or destroyed can be addressed to the DPO or Headteacher.

The consequences of getting data security wrong can be very serious for our most vulnerable data subjects and breaches of data protection may be subject to disciplinary action and further subject to legal action or criminal prosecution.

10.3 Email

All staff are expected to adhere to the good practice around the use of email set out in the current Information and Records Management Society 'Schools Toolkit' understanding their role and responsibilities with regard to:

- the 8 things they must know about email including that it is not always a secure medium to send confidential information by, that email is disclosable under the Freedom of Information Act 2000, that any employer has a right to monitor the use of email under the Regulation of Investigatory Powers Act 2000, and that email is one of the most common causes of stress in the workplace.
- creating and sending email.
- sending attachments.
- using disclaimers.
- managing received e-mails; and
- retaining emails.

Others who have legal obligations to us because they process data that we control will be made aware of our email protocols as necessary.

All staff are required to use the authorised email disclaimer as follows:

> *This e-mail may contain confidential information (which may also be legally privileged) and is intended solely for the use of the intended named recipient. If you are not the intended recipient you may not disclose, copy, distribute or retain any part of this message or its attachments. If you have received this message in error please notify the originator immediately by using the reply facility in your e-mail software. Incoming and outgoing emails may be monitored in line with current legislation. All copies of the message received in error should be destroyed.*

10.4 Generative Artificial Intelligence

This emerging technology:

- stores and learns from the data it is given – this means that any data entered should not identify a living person
- can create believable content, including more credible scam emails requesting payment – research has shown that people interact with generative AI differently than with humans and the content may seem more authoritative and believable.

This school is committed to:

- ensuring we make decisions about using generative AI for the first time ever or using it in completely new ways, by employing the privacy by design approach outlined in section 6 to promote privacy and data protection compliance from the start
- carrying out a DPIA if we feel that new projects or tasks involving generative AI could create a high risk to individuals' interests
- protecting personal and special category data in accordance with data protection legislation
- ensuring all staff receive enough basic information, instruction, training and/or supervision to enable them to work safely with generative AI and without significant risks to their or pupils' health, including mental health e.g., using Cyber Security for Schools - NCSC.GOV.UK and keeping staff updated on emerging risks, recognising and managing them using NSCS blog articles ChatGPT and LLMs: what's the risk and the principles for the security of machine learning
- not allowing or causing intellectual property, including pupils' work, to be used to train generative AI models, without appropriate pupil, student or parental consent or exemption to copyright

- regularly reviewing our cyber risk assessment and strengthening our cyber security to address professional advice we receive, incidents, or changes in risks that we become aware of e.g., generative AI could increase the sophistication and credibility of cyber attacks
- ensuring that children and young people are not accessing or creating harmful or inappropriate content online using generative AI in line with keeping children safe in education in terms of:
  - what staff need to do to protect pupils and students online
  - how they can limit children's exposure to risks from the school's IT system

  For more information about this, see our Online Safety Policy ensuring we have appropriate systems in place in line with DfE filtering and monitoring standard to block or restrict harmful content and to help us prevent the misuse of generative AI e.g., to bully others.

All staff have a responsibility to identify when their activities involving generative AI imply the need for a DPIA. This could be doing an entirely new task using generative AI, or it could be changing the way a well-established task is being done to involve AI.

Staff must consult the Headteacher and receive agreement to their plans in writing before using generative AI tools to create original content by pupils or produced from their original work in a new or significantly different way from established practice.

10.5 Transfers of data outside the UK

Transfers of personal data outside the UK are treated differently depending on which countries it is being transferred between or through, what is being transferred, why and how, and how closely those countries' approaches to data protection align with the UK's.

We will follow current ICO guidance on International transfers after the UK exit from the EU Implementation Period and Standard Contractual Clauses (SCCs) after the transition period ends for country specific requirements when we need to transfer personal data internationally.

Regarding transfers between the UK and the EU:

When the UK left the EU on 31 January 2020 it entered a "transition" period which kept existing UK-EU data transfer rules aligned as if the UK were still part of the EU ('frozen GDPR'). This allowed freedom of movement for data to continue to flow as before.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED) i.e. it was agreed that the UK as a third country to the EU ensures an adequate level of protection of the rights and freedoms of EU data subjects to allow transfers. This means that data (excluding data transferred from the EU to the UK for the purposes of UK immigration control) can continue to flow as it did before, in the majority of circumstances until 27 June 2025.

Following the above ICO guidance allows us to continue to meet our data protection obligations. We will also refer new or uncertain international transfers of personal data to or from the UK to our DPO when making decisions about the safety, security, and lawfulness of transferring it.

10.6 Record keeping

The legislation contains some explicit provisions about documenting our processing activities but that is not the reason we keep records. We need to know what data we have and how we use it to be able to control it effectively; we need to be able to justify our decisions about data; and we may need to provide evidence to the ICO as part of a data breach investigation.

We use the ICO GDPR Documentation Template to fully comply with the record keeping required of us under Article 30. It is the responsibility of all staff to ensure the spreadsheet remains a current reflection of how they work with data. Changes in practice should be reported to the Headteacher.

We also keep records of our DPIAs, consent, staff training, and our contracts and data sharing agreements i.e., our employment and service provision contracts, processor contracts, and joint-controller data sharing agreements.

We also keep some simple logs which briefly detail:

- SARs.

- other types of data requests and what we did e.g., objection, rectification, withdrawal of consent, education record request etc.
- data destruction.
- breaches.

All staff are made aware of our record keeping obligations and some staff are specially trained in managing them.

11. Data Sharing

We are required to share personal data with some organisations by law e.g., our census data with the DfE. At other times we share information to improve or protect people's lives and we have included information about this in our Privacy Notices.

All staff are expected to make reference to the current ICO Data Sharing Checklist in making decisions on whether to share data or not and how to do it. Unless the data sharing is routine and pre-authorised e.g., medical data routinely disclosed to the outdoor adventure centres we go on residential trips to, no decision should be made regarding the disclosure of any sensitive personal or sensitive commercial data without reference to an immediate line manager or the Head teacher. If nobody involved in the decision-making has received suitable training in data protection, the DPO must be consulted before data is disclosed externally.

With regard to the disclosure of child protection data, we will always follow the current *'Information Sharing Protocol'* available from our Local Children's Safeguarding Partnership.

We have simple procedures in place regarding unavoidable disclosures to people we do not already have data processing or data sharing agreements with e.g., to an engineer during emergency repair of a computer system, which includes a requirement for them to sign a suitable non-disclosure agreement.

12. Data Retention

We can only keep personal data for as long as we need it. How long that is will depend on the circumstances and the reasons we obtained it.

We will generally follow the guidelines set out in the current Information and Records Management Society 'Schools Toolkit' and we will specifically follow requirements placed on us by our Local Authority and Local Children's Safeguarding Partnership in particular.

We typically retain pupil data and data about their family and other involved professionals until they leave us. Otherwise, we retain it for a few days or weeks e.g., trip consent forms, or for 3-50 years depending on whether it is education related or incident related.

We typically retain workforce data for between 6 months and 25 years after an event or the end of their employment with us, depending on their role or if they may have been affected by changes to employment or pension terms ruled by the courts as unlawful. Some pieces of data may need to be retained for 50 years such as records of potential exposure to asbestos, and some indefinitely such as a personnel file when there have been allegations.

We typically retain the personal data of contractors and other professionals in line with work done or contractual agreements, and longer in cases of dispute or allegations.

Some information is retained for more indefinite periods e.g., outreach programme take-up data so that we can analyse trends, or event photographs and accounts so that we can maintain a historical record.

13. Data Disposal

We will dispose of all paper and digital data securely when it is no longer required.

A Destruction Log will be kept of all data that is disposed of. The log will include any document ID, classification, date of destruction, method, and authorisation.

14. Breach Reporting

Any breach of this policy or of data protection laws must be reported to the DPO as soon as practically possible i.e., as soon it becomes apparent. We have a legal obligation to report any qualifying data breaches to the ICO within 72 hours.

A qualifying data breach is one where, if not addressed in an appropriate and timely manner, it could result in physical, material or non-material damage to someone such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to them.

If we experience a data breach and we are unsure whether it is a qualifying data breach that must be reported to the ICO, we will use the ICO self-assessment tool to decide.

All staff and anyone else who owes us or our data subjects a legal duty, a duty of care, or a duty of confidentiality have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary.
- maintain a register of compliance failures.
- notify the individuals affected; and
- notify the ICO of any compliance failures that are material in their own right or part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures may be liable to disciplinary action. Where others have been involved in a data breach, a report will also be made to their employer or DPO if relevant to the breach.

15. Our Obligations to our Data Processors

As the data controller we have obligations to our data processors when we give them the personal data of our data subjects which include in general, but are not limited to responsibilities to:

- provide accurate personal data and all necessary corrections in a timely manner.
- employ appropriate technical and organisational security measures when providing and using the personal data being processed.
- only request user access to the data processing for employees and the contractor at a level commensurate with their work tasks and responsibilities e.g., have the fewest possible users who are authorised and enabled to access the accident & incident reporting system which contains sensitive health data.
- respond promptly to requests from our processors for data updates and provide updated and accurate written instruction regarding the continued access to data that we require.
- require our users of any data processor's system to comply with strict password security measures e.g., length, complexity, not shared etc.
- take appropriate action regarding any breaches.
- ensure our users of a processor's system website understand their responsibilities with regard to the DPA and the GDPR. Anyone found to have carried out unauthorised or unlawful processing activities must be made aware that they will be subject to disciplinary action by you and may be further subject to legal action or prosecution.
- inform our processor as immediately as possible if:
    - we need to remove security access i.e., to our data on their system, from individuals who no longer have any legal right or authority to access it e.g., employees who have left our employment,
    - we need their assistance to comply with a Subject Access Request,
    - we need them to stop processing the personal data of any of our data subjects,
- be sure of our grounds under the law for asking a processor to stop processing the personal data of any of our data subjects and that they are compatible with other applicable laws or legal rights,

- be very sure of our grounds to erase data under the law because we can expect to pay the full costs of any extraordinary measures required to recover erased data where we have failed in our duties.

All staff involved in using the data that we control with the processing services that we contract with have a duty to meet all of our conditions of service. Queries about our contracts for processing activities should be addressed to the Headteacher.

Data Classifications and Handling Requirements

This is an indicative rather than exhaustive guide to data classification and the resulting data handling requirements. All relevant queries should be directed to the Data Protection Officer or the school office.

	Public	Confidential	Sensitive
Impact if the information becomes public	**No risk**	**Low-Medium Risk** May result in minor reputational or financial damage to the school. May result in minor privacy breach for an individual.	**Medium-High Risk** Could substantially damage the reputation of the school, have a substantial financial effect on school or a third party, or would result in a serious privacy breach to one or more individuals.
Description of the information	Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain.	May result in minor reputational or financial damage to the school. May result in a minor privacy breach for an individual. Information that should only be available to sub-groups of staff within the school who need the information to carry out their roles.	Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.
Examples of information This list is indicative not exhaustive if unsure ask the Headteacher for advice	● Prospectus ● Press releases ● Open content on the school web site ● Publicity flyers and leaflets ● Published information released under the Freedom of Information Act ● Policies, annual reports, and financial statements ● Job adverts (excluding internal only positions) ● staff names and contact details ● Staff publications. ● Agendas and minutes of school committees and working groups (except reserved business). ● Patented intellectual property.	● Student personal details e.g., demographics, personal email address etc. ● Staff personal details e.g., demographic, payroll number, personal email address etc. ● Internal only school policies, processes, and guidelines. ● Internal only job adverts. ● Tender bids prior to award of contract ● Individual's salaries ● Student's assessment marks. ● Job application responses/CVs (unless they contain sensitive personal information).	Sensitive personal data and some other data. ● Exam questions prior to use ● Medical records ● UPRNs ● Usernames and passwords ● Investigations/disciplinary proceedings. ● Payment card details. ● Financial information (banking details and data not already disclosed in financial statements). ● Passwords and access codes to school systems. ● Some complaints or requests ● Biometric data
Security Marking	No marking required	Must be clearly marked as **Confidential**	Must be clearly marked as **Sensitive**

Appendix A

	Public	Confidential	Sensitive
Storage (electronic)	● Store using school IT facilities to ensure appropriate management, back-up, and access. ● Use only the school approved cloud service. Some cloud services may **not** be used because they link to computer C: drives which is not secure.	● Store only on the school IT network and never on the C: drive of a PC/laptop (beware downloading information when a laptop is not connected to the school domain - the download will go onto the C: drive and you may be in breach of this policy). ● Store only on the C: drive of a specially encrypted PC/laptop. ● Store only on the approved cloud service in a suitably restricted folder. ● Portable devices such as USB sticks must be encrypted and must **not** be used for long term storage due to the risks of loss or corruption of data. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any unencrypted school device e.g., tablet, laptop, mobile phone etc.	● Store only on the school IT network in rigorously monitored & restricted access drives. ● Never to be stored on the approved cloud service unless also separately encrypted. ● Never to be stored on any portable storage device i.e., USB drive regardless of encryption. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any school device e.g., tablet, laptop, mobile phone etc. unless it has been specially encrypted *and* there are other high level procedural safeguards.
School Website	No restrictions	Not permitted	Not permitted
Storage (hardcopy)	No restrictions	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.
Email hosted by school	No restrictions	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g., telephone. Emails to internal recipients i.e., school email account-to-school email account are secure, so encryption and encrypted attachments are not necessary.	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g., telephone. Emails to internal recipients i.e., school email account-to-school email account are secure, so encryption and encrypted attachments are not necessary.
Personal email account e.g., Hotmail etc.	No restrictions	Not permitted	Not permitted
Post (Internal)	No restrictions	In a sealed envelope marked Confidential.	Seal envelope, mark Confidential & hand deliver.

Appendix A

	Public	Confidential	Sensitive
Post (External)	No restrictions	Tracked and recorded delivery only and marked Confidential	Tracked and recorded delivery only and marked Confidential within two separate envelopes.
School-based server	No restrictions but consideration should be given to back-up requirements.	No storage or creation is permitted unless the server environment is equivalent to the school-based server or the CTU server environment.	No storage or creation permitted unless the server environment is equivalent to the school-based server or the CTU server environment.
School owned laptop	No restrictions but do **not** use to store master copies of vital records.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.
Personally owned mobile device	No restrictions	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.	Not permitted unless authorised by the Senior Information Risk Owner (SIRO). Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.
School owned desktop (public areas)	No restrictions, but always lock the screen when unattended.	Not permitted. The risk of incidental disclosure is too high.	Not permitted. The risk of incidental disclosure is too high.
School owned desktop (key/card access-controlled areas)	No restrictions, but always lock the screen when unattended.	Only permitted on encrypted drives or using or password protected files. Always lock the screen when unattended.	Only permitted on encrypted drives. Always lock the screen when unattended.
School owned mobile device	No restrictions, but always lock the screen when unattended.	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document.	Not permitted unless authorised by the SIRO. Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document
Removable media (CDs, USB drives etc.)	No restrictions.	Encrypted storage with strong password e.g., 8 characters or longer and a mixture of uppercase, lowercase, digits, and special characters.	Encrypted storage with strong password e.g., 8 characters or longer and a mixture of uppercase, lowercase, digits, and special characters.
Disposal	No restrictions. Recycle where possible.	Shred or place in a confidential waste bag. Delete from electronic media when no longer required.	Cross shred only & put shredded material into the confidential waste. Appropriately scrub data from devices. Some devices (encrypted USB drives) may need to be securely destroyed. Seek advice from the IT manager.