



HILPERTON C of E PRIMARY SCHOOL
DATA PROTECTION AND SECURE DATA HANDLING
POLICY RATIFIED ON: 7th July 25
POLICY REVIEW DATE: July 27



This policy should be read and understood in conjunction with the following policies and guidance:

- [The UK General Data Protection Regulation guidance and resources \(UK GDPR\)](#)
- [The Data Protection Act 2018 \(DPA\)](#)
- [Data Protection in schools \(DfE February 2023\)](#) <https://www.gov.uk/guidance/eu-exit-guide-data-protection-for-education-providers>
- [Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers \(DfE May 2024\)](#)
- [Privacy notices: an explanation of privacy notices \(DfE 08/24\)](#)
- [Data protection: privacy notice model documents](#)
- The school's policies on:
 - Equality Policy
 - Online Safety Policy
 - Remote Learning Policy
 - Safeguarding and Child Protection Policy
 - Code of Conduct for Staff
 -

APPENDICES:

Appendix 1	Privacy Notice to pupils
Appendix 2	Privacy Notice to parents
Appendix 3	Privacy Notice to school staff
Appendix 4	Privacy Notice to school governors
Appendix 5	Data Protection: toolkit for schools (DfE August 2018 updated Feb 2023)
Appendix 6	Information Asset Register
Appendix 7	Data Subject Access Requests
Appendix 8	https://ico.org.uk/for-the-public/official-information/ https://www.gov.uk/make-a-freedom-of-information-request

CONTENTS:

1. General Principles
2. Key Definitions
3. Requirements under the current legislation
4. Responsibilities
5. Rights of individuals on whom data is held
6. Data protection and children
7. Privacy notices
8. Documentation
9. Accountability and governance
10. Personal Data Breach



11. Securing and handling data
12. Freedom of Information
13. Review of policy

1. General Principles:

- We recognise that schools have increasing access to a wide range of personal data about pupils, parents¹ and staff, some of which we are legally required to gather and process in order to carry out our duties as a public authority, but also to support the development of pupils (educationally, socially and emotionally), to protect the pupils in our care and to facilitate the efficient running of the school.
- Data and records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability.
- Under the UK Data Protection Legislation (as listed above) there are strict legal guidelines in place as to how data should be both 'controlled' and 'processed', which the school is fully aware of and complies with.
- The UK GDPR sets out 7 key principles regarding the processing of personal data which are:
 - lawfulness, fairness and transparency
 - purpose limitation
 - data minimisation
 - accuracy
 - storage limitation
 - integrity and confidentiality (security)
 - accountability
- These regulations apply to 'personal data', 'special categories of personal data' and personal data relating to 'criminal convictions and offences'.
- This policy applies to all data and records created, received or maintained by staff of the school in the course of carrying out its functions.

2. Key Definitions (please click on any links for more detailed information):

- **Records** are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or maintained in hard copy and/or electronically.
- **Personal data** is defined in the GDPR as "any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, local data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental economic, cultural or social identify of that natural person."
- In our school, examples of personal data include:
 - identity details (e.g. name, 'unique pupil number (UPN), title or role)
 - contact details (e.g. address, telephone number, email address)
 - information about pupil behaviour and attendance
 - assessment and exam results
 - staff recruitment information
 - staff contacts

¹ **Parent/s** refers to birth parents and other adults who are in a parenting role, for example step-parents, foster carers and adoptive parents.



- staff development reviews
- staff and pupil references
- **Special categories of personal data** relates to personal data that needs more protection because it is sensitive and specifically refers to information held about an individual in the following categories:
 - racial or ethnic origins
 - political opinions
 - religious or philosophical beliefs
 - trade union membership
 - genetic information
 - biometric information (where used for identification purposes))
 - health matters (e.g. medical information)
 - sex life
 - sexual matters or sexual orientation
- In our school, we also treat as special category data any personal data about:
 - a safeguarding matter
 - pupils in receipt of pupil premium
 - pupils with special education needs and disability (SEND)
 - children in need (CIN)
 - children looked after by a local authority (CLA)and, as this data, by its very nature could create more significant risks to a person's fundamental rights and freedoms, there are additional safeguards in place.
- **Criminal offence data** is personal data that's treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures. Criminal offence data includes:
 - the alleged committing of an offence
 - the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing.Schools process criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means that the school is processing criminal offence data. This applies even though the check has not revealed any conviction.
- **Commonly used data format** means the format in which the data is stored must be widely used and well-established
- **Data assets:** Schools hold personal data in several forms. These are commonly known as its data assets. Data assets comprise:
 - data items (single pieces of information)
 - data item groups (data items about the same process)
 - data sets (collections of related data that can be manipulated as a unit by a computer)
 - systems (administrative software)
 - systems groups (the larger systems housing administrative software)
- **Data controller:** The school is the 'data controller' for most of the personal data we collect, store and use. This means that we are responsible under the Data Protection Act 2018 for protecting data in every situation where we decide:
 - whose information to collect
 - what type of data we need and why we need it
 - whether the data can be shared with a third party
 - when and where the data subjects' rights apply
 - how long we keep the data



Where we are required to supply a copy of some personal data to the Department for Education (DfE) the DfE also becomes an independent data controller of the copy it receives.

- **Data subjects:** Schools collect, store and use personal data about a variety of individuals. In this context, those individuals are known as 'data subjects'. A schools' data subjects include:
 - pupils and former pupils
 - parents
 - employees and non-employed staff
 - governors
 - local authority personnel
 - volunteers, visitors and applicants
- **Data processors** are responsible for processing personal data on behalf of a controller.
- **Data protection impact assessments** are required when introducing new technology for the handling and processing of personal data and when data is processed on a large scale. They are required under GDPR legislation whenever the processing of personal data is likely to result in a 'high risk to the rights' and freedoms' of an individual. Their aim is to assess the level of risk involved and the security measures that need to be put in place to consider and mitigate risks to individual privacy to provide individuals with reassurance and demonstrate both accountability and compliance with data protection law.
- **Information Commissioners Office (ICO)** is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
- **Personal data breaches** are defined as a security incident that results in personal data at a school being:
 - lost or stolen
 - destroyed without consent
 - changed without consent
 - accessed by someone without permission.Data breaches can be deliberate or accidental. A breach is about more than just losing personal data.
- **Staff** includes all staff employed by the school in any capacity, governors and volunteers
- **Structured Data** is data which can be extracted by software (e.g. from a spreadsheet) as is therefore normally machine readable.
- **Subject Access Requests (SARs)** give individuals the right to see a copy of the information an organisation holds about them
- **Third countries** is any country outside the United Kingdom
- **Unstructured data** is the **collective name for the information that an organisation creates, and keeps**, to help it carry out its primary tasks, but isn't in a recognisable structure or contained in a database

3. **Requirements of UK General Data Protection Regulations (UK GDPR)**

- **Under Article 5 of UK GDPR** the data protection principles set out the main responsibilities for organisations which require that personal data shall be:
 - a) processed lawfully, fairly and in a transparent manner in relation to the individuals (lawfulness, fairness and transparency)
 - b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purpose ('purpose limitation')



- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- e) kept in a form which permits identification of the data subjects for no longer than is necessary for the personal data to be processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes subject to the implementation of the appropriate technical and organisation measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
- f) processed in a manner that ensures appropriate security for the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality')

4. **Responsibilities:**

The school as the data controller for most of the personal data we collect, store and use. The school is responsible for protecting data in every situation where it decides:

- whose information to collect
- what type of data it needs and why it needs it
- whether the information can be shared with a third party
- when and where data subjects' rights apply
- for how long the data should be kept

The school:

- also has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment and the person with overall responsibility for this policy is the Head Teacher (for more detail see sections below on '**Documentation**' and '**Accountability and Governance**')
- is required to appoint a Data Protection Officer (DPO) to oversee the collection, processing and security of data. Hilpertons C of E Primary School has appointed One West as its DPO, and they can be contacted by email at:

- - One West (Bath and North-East Somerset Council) Email: i-west@bathnes.gov.uk*
 - Guildhall, High Street, Bath, BA1 5AW Telephone: 01225 395959*

- as both a controller and processor of personal data, has a responsibility to register with the 'Information Commissioner's Office' and to renew the registration annually
- must inform pupils, parents, staff and governors (through the issuing of **Privacy Notices** – see section below) what data they are required to collect and retain and the lawful basis for processing personal data as defined in section 3 above.
- must, through the same Privacy Notices also inform pupils, parents, staff, and governors of any special category data and/or data on criminal convictions or offences, they hold, together with the lawful basis for that processing that data'
- follows the guidance with regard to information sharing of data related to safeguarding and child protection as set out by the Department of Education (DfE) [Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers \(DfE May 2024\)](#)



- must produce and maintain, through an annual audit an 'Information Asset Register' detailing all data that it holds (see section 7 below).

Governors

The responsibility and accountability for compliance sits with the governors. Therefore, governors should check that the school:

- monitors their data protection performance
- supports the data protection officer
- has good network security infrastructure to keep personal data protected
- has a business continuity plan in place that includes cyber security

Senior leaders are accountable for:

- deciding how the school uses technology and maintains its security, including the use of generative AI
- deciding what data is shared and how
- setting school policies for the use of data and technology
- understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate
- assuring governors that the school has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive annual training on data protection, including specific school processes such as personal data breach reporting processes and the escalation of information rights requests.

The Data Protection Officer (DPO):

The Data Protection Officer (DPO) is the first point of contact for external supervisory authorities as well as those individuals (pupils, staff and parents) whose data the school holds. In addition, the DPO is responsible for:

- advising school leaders and staff about their data obligations on an ongoing basis and also as part of the staff induction process
- understanding and informing all staff on the potential data protection risks of using generative AI in schools and the difference between 'open' and 'closed generative AI
- monitoring compliance
- conducting regular data audits to ensure that data is only kept for as long as it is needed as in line with the requirements clearly set out in the DfE guidance on 'Data protection in schools'
- ensuring that data is disposed of securely and confidentially in line with the guidance issued by the ICO ([practical methods for destroying documents that are no longer needed](#))
- developing and updating data protection policies and procedures
- monitoring who in the school has access to personal data
- advising when [data protection impact assessments](#) are needed and that they are carried out in line with DfE guidance
- answering data protection enquiries from staff, parents and pupils
- making sure privacy notices are regularly reviewed and updated
- supporting and advising staff who have data protection queries
- communicating with the Information Commissioner's Office (ICO)
- reporting to the governing board about data protection
- advising the governing board on data protection risks
- advising on and co-ordinating responses to information rights requests
- making sure all assets containing personal data are appropriately managed and secure



- ensuring that when a DPIA concludes that there is a high risk, which cannot immediately be mitigated against, the ICO is consulted **before** any such data is processed
- ensuring that the Information Asset Register is kept up to date and that staff are involved in an annual audit of its contents in relation to the files that they hold

Individual staff and employees:

- **All staff should be aware of what:**
 - personal data is
 - 'processing' means
 - their duties are in handling personal information
 - the processes are for using personal information
 - is permitted usage of that data
 - the risks are if data gets into the wrong hands
 - their responsibilities are when recognising and responding to a personal data breach
 - the process is for recognising and escalating information rights requests
- **In addition, all staff** must contribute to the annual review of the Information Asset Register by advising the DPO of any additions or deletions from the register of records that they hold.
- **Any staff in school who create and store data, enter data into applications or software, decide if and when they'll process certain data, and handle paper documents are responsible for:**
 - making sure they have a legitimate need to process the data
 - checking that the data they store is needed to carry out necessary tasks
 - identify any risks and understanding the governance arrangements that oversee the management of risks.
- Staff are also responsible for making sure that pupils using personal data for projects or coursework do so appropriately. This includes being compliant when storing data.

Parents, pupils and staff: should ensure that the information they provide the school with is accurate and kept up to date.

5. Rights of individuals on whom data is held

- The UK GDPR identifies 7 'rights' of individuals on whom data is held, some of which apply to schools and others which are aimed at commercial practices. In this policy we have given a summary of the guidance regarding each of these rights, but should you wish for more detailed information, this can be found on the ICO website or by clicking on the links below. You can also obtain hard copies of these documents from the school office. The 7 rights as outlined by the UK GDPR are:
 - [right to be informed](#)
 - [right of access](#)
 - [right to get your data corrected](#)
 - [right to erasure](#)
 - [right to restrict processing](#)
 - [right to data portability](#)
 - [right to object](#)
- Some of these rights may not apply, depending on the legal bases on which we hold and process the data.
- An individual can make a request regarding any of the areas listed above, either verbally (face to face or on the phone) or in writing (i.e. email, letter or via social media) and they need not be directed towards a specific person or contact point. However, we would encourage any



individual wishing to exercise their rights to put their request in writing and/or speak directly to the DPO or a member of the school's senior management team. Where the request is made electronically, the school will provide the information requested in a commonly used electronic format unless you request us to supply it in another form.

- A third party can also make a Subject Access Request (SAR) on behalf of another person as long as the school has received confirmation that the third party has their permission. The school will ask for proof such as written permission from the subject in question or a power of attorney document.
- We have timescales in place to provide individuals with a response to any of the request they make but there may be exceptional circumstances (e.g. school closures) where it is not always possible to adhere to these time schedules. Where this is the case, individuals will be kept informed.
- The school reserves the right to refuse to respond to a request when they are manifestly unfounded or excessive, especially if they are repetitive. In such cases, the individual making the request will be informed of the school's decision not to comply together with the reason why, as well as informing them of their right to complain to the supervisory authority without delay and at the latest within one month.
- In all cases we will justify our decision in writing and a copy will be kept on the school's files.
- Much of the data that schools are required to collect and process falls under our duty as a public authority in order for us to fulfil our legal obligations, and this basis is referred to as our 'public task'. In addition, we also hold data on other bases (as outlined in our Privacy Notices) namely, 'contract' (in relation to the staff we employ) 'consent' 'legitimate interests' and 'vital interests'. The table below shows the rights that apply in 3 areas.

LAWFUL BASIS	RIGHT TO ERASURE	RIGHT TO PORTABILITY	RIGHT TO OBJECT
Public Task	X	X	✓
Contract	✓	✓	X
Consent	✓	✓	X
Legitimate Interests	✓	X	✓
Vital interests	✓	X	X

Right to be informed: (Please also refer to the section below on 'Privacy Notices'.)

- At the time of requesting data from individuals (pupils, parents, staff, governors), the individuals must be informed of their rights regarding that data, which should include:
 - the name and contact details of the school's Data Protection Officer
 - the categories of personal data
 - the school's purpose and lawful process/es for processing data the categories of personal data being requested
 - the legitimate interests that apply where that is the lawful basis
 - who the data is shared with
 - the details of the transfer of personal data to any third countries or international organisations (if applicable)
 - how long it is held for
 - the right to withdraw consent at any time (where relevant depending on the lawful basis)
 - the right to lodge a complaint with a supervisory authority (the ICO)
 - whether the provision of personal data is part of a statutory requirement and the possible consequences of failing to provide the personal data



- the existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences
- In the event that it becomes necessary for us to process personal data in a way that has not been detailed in the privacy notice already received, we will ensure that we bring this change to the attention of all individuals involved before we start processing.
- Where we have obtained personal data from another source (e.g. outside agency or another school) we will provide the individuals concerned with the necessary privacy information within a reasonable period of obtaining the data and no later than one month from receiving it.
- In addition, there may be times during the school year when we may require further information from you for a specific purpose. At that time, we will advise you of any additional information regarding your rights as we are required to do by UK GDPR. If we are reliant on 'consent' as our lawful basis, you will be advised of that and you will be required to give your consent in writing.

Right of access:

- All individuals have the right to access their personal data and supplementary information and this is referred to as a '[Subject Access Requests \(SARs\)](#)'. Appendix 7 gives more information (click on the link).
- The right of access allows individuals to understand how and why we are holding their data and to check that we are doing it lawfully.
- This right of access can also be exercised by a child, even if they are under the age of 13. However, before responding to any such request, we retain the right to consider whether or not the child is mature enough to understand their rights. More detailed information can be found in section 6 below.
- The information that we provide in response to any request will be in a concise, transparent, clear and easily accessible form. This will be particularly important where the information is addressed to a child.
- Individuals have the right to be provided with a copy of the information that is held on them free of any charge unless the request is manifestly unfounded, excessive² or repetitive, in which case the school reserves the right to charge a reasonable fee, based on the administrative costs of providing that information. Should this be the case, individuals will be advised of any charges in advance and the school is not required to comply with the request until the fee has been received.
- A reasonable fee may also be charged for further copies of the same information.
- Information must be provided without delay and at the latest within one month of receipt of the request or longer depending on when the request is made (see final bullet point). However, this deadline can be extended should we have to wait for the requester to provide identification, authority or any additional clarification we might need.
- Where the requests are complex or numerous, the school can extend the compliance period for a further two months as long as the individual requesting the information is informed that this will be the case within one month of the receipt of the request. The school will, at the same time, explain why this extension in time is necessary.
- If a SAR is received on the last day of the school term or during the school holidays, we are still required to respond within one calendar month. However, if there is any reason why this cannot be done, we will inform the requester as soon as possible.
- Where we hold a large amount of personal data about an individual, we can ask that the request be specific.

² As defined in the ICO guidelines in each section on 'rights' – please click on the link for any of these sections and scroll down for more information.



- If, by responding to a SAR we would also have to disclose information about another individual who could be identified from the information supplied, we do not have to comply with the request unless the other individual has given their consent, or it is reasonable for the school to proceed without their consent.
- Where we believe that the SAR is manifestly unfounded (e.g. an individual submitting multiple SARs with malicious intent) we can refuse to comply with the request. Further information on this can found in the section entitled 'Sharing personal data' in the DfE document '[Data Protection in schools](#)'.

Right to get your data corrected:

- Individuals have the right to have their personal data corrected if it is inaccurate or incomplete.
- Where the school has disclosed this information to a third party (e.g. Department for Education or Local Authority) it is responsible for ensuring that the third party also corrects the data in question. The individual will be advised of any third parties to whom the data has been supplied, where appropriate.
- The school must ensure that data is rectified within one month, but we may extend this period for a further two months where the request is complex.
- Where the school decides not to take action to rectify data at the request of an individual, we will explain why and inform them of their right to complain and to whom that complaint should be addressed.
- Individuals may request a restriction of the processing of their data where they are contesting its accuracy and the school are checking it and, as a matter of good practice this request should be complied with even if the individual has not exercised their right to restriction (as detailed below)

Right to erasure:

- Individuals have the right to request that their information is erased/deleted where there is no compelling reason for its continued processing i.e.:
 - where it is no longer necessary for the school to hold that data (bearing in mind the requirement to retain certain documents for a specific period of time)
 - when, if the data is obtained under the basis of 'consent' that consent is subsequently withdrawn
 - where data has been unlawfully processed or where an individual objects to the processing and there is no overriding legitimate interest for the processing to continue.
- This right to erasure does not apply when:
 - we require the data to fulfil our legal obligations
 - 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 its erasure will impair those processes, and
 - for the establishment, exercise or defence of legal claims.
- The school has one month to respond to a request.
- In most cases we cannot charge a fee to comply with a request for erasure, but we can charge a 'reasonable fee' for the administrative costs of complying with a request we believe to be manifestly unfounded or excessive, in the event that we agree to respond to that request. In such circumstances, we will not proceed until the fee has been received.

Right to restrict processing:

- In certain circumstances, individuals have the right to request the restriction or suppression of their personal data, which means that they can limit the way in which any organisation uses their data (as opposed to asking for their data to be erased). This right applies when:



- an individual contests the accuracy of the data being processed and you are verifying the accuracy of that data
- an individual believes that data has been unlawfully processed but opposes erasure and requests restriction instead
- the school no longer needs to keep the data but has been asked to do so in order to establish, exercise or defend a legal claim
- an individual objects to the processing of the data and the school is considering whether its legitimate grounds override those of the individual in question.
- Where the school has disclosed this information to a third party (e.g. Department for Education or Local Authority) it is responsible for ensuring that the third party also restricts the processing of the data in question, albeit temporarily. The individual will be advised of any third parties to whom the data has been supplied, where appropriate.
- We will justify our decision for any action we take in writing. In the event that we do refuse to comply or wish to charge a fee, individuals will be informed within one month of the receipt of the request (with exceptions being made for school holidays) and will advise individuals of our reasons, their rights to make a complaint to the ICO and their rights to seek a judicial remedy.
- Should the school decide it is appropriate to charge a fee or believe that we require additional information to identify an individual, no further action will be taken before that fee is received, after which the school still has one month to respond.

Right to data portability:

- The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller. The right to data portability only applies when:
 - the information in question has been provided by an individual to the school
 - the data format is 'structured', 'commonly used' and machine readable (see definitions above)

Right to object:

- Where applicable, individuals have the right to object on "grounds relating to their particular situation".
- Where an individual exercises their right to object, we are required to stop processing the personal data we hold 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.
- When an individual objects to the processing of data based upon a public task (including scientific or historical research) or legitimate interest they must give specific reasons why they are objecting to the processing of the data and these reasons should be based upon their particular situation.
- The school can refuse to comply if the processing is for the established, exercise or defence of legal claims.
- Individuals are advised on their right to object in our Privacy Notice
- The school has one calendar month to respond to an objection

6. Data protection and children

- Children need particular protection when collecting and processing their personal data as they may be less aware of the risks involved, particularly when you are relying on 'consent' as the lawful basis, especially for any online service. In such cases, only a child over the age of 13 can give consent.



- In the majority of cases, the data we collect on children does not rely on consent as the lawful basis, but we need to ensure that in any correspondence with children, the language we use is clear and unambiguous.
- For children under the age of 13, we will treat the request in the same way as we would if an adult made it, provided there are no issues with competency. Parents can also make a SAR on behalf of a young person. If a child is 13 or over, schools must check whether they are happy for their personal data to be shared with their parent.
- We will not respond directly to a request from a child if we believe that: they do not have the maturity or competence to act independently; have a health condition that limits their understanding or have given consent for a representative or someone with parental responsibility to act on their behalf
- Children have the same rights as adults over their personal data, including all the rights outlined above. Where a child is not considered to be competent, an adult with parental rights may usually exercise the child's data protection rights on their behalf.

7. Privacy Notices:

- The school, in compliance with the requirements of the UK GDPR, will issue Privacy Notices to all individuals on whom we hold data, at the time that they join our school, namely:
 - pupils (via their parents),
 - parents
 - staff
 - governors
- (See Appendices 1, 2,3 and 4 Copies of our Privacy Notices to pupils and parents can also be found on the school website.
- Privacy notices will be updated from time to time as a response to advice received from the Department of Education. When this is the case, the updated notice/s will be published on the school website and parents will be notified.
- Our Privacy notices will contain the following information:
 - the categories of data that we hold
 - why we collect it
 - the lawful basis on which we process that data
 - who we share the data with
 - how long we retain the data
 - your rights in relation to your data, including the right to withdraw consent, where that is the lawful basis.
 - who to contact regarding any aspect of the data held and how to complain over concerns about the way the data is being used.

8. Documentation

- The UK GDPR contains explicit provisions regarding what we are required to document regarding the data we control. UK GDPR legislation states that we must document the following information (available both in electronic form on our website and as a paper copy, which can be obtained by request from the school office):
 - the name and contact details of our organisation
 - the contact details for our data protection officer
 - the purpose of our processing
 - descriptions of the categories of individuals and categories of personal data who receives the personal data we process
 - our retention schedules (based on DfE guidance)



- a description of our technical and organisational security measures (Appendix 5)
- Our Information Asset Register (as referred to above) records the following information:
 - descriptions of the data that we hold (personal data, special category data and data relating to criminal convictions and offences)
 - the lawful basis for our processing with reference to Articles 6, 9 and 10 of the UK GDPR
 - in what format and how that data is held
 - how long we retain the data for
 - how it should be disposed of

9. Accountability and governance

- Under the UK GDPR, the school is required to demonstrate that we comply with the principles of the accountability and responsibility and in order to do this we must ensure that we implement appropriate technical and organisation measures which will include:
 - publication of this policy
 - on-going training for staff and induction for new staff
 - internal audits of our processing activities, including data protection impact assessments for personal and/or special category data that is processed on a large scale
 - internal audits of all the personal data we hold, including special categories of personal data which include the form that the data is held in, where it is held, who has access to it, the security measures in place and how long it is retained for
- We will also:
 - ensure that records are kept securely, in line with our legal obligations
 - ensure that records are disposed of securely in line with our legal obligation
 - ensure that our records are kept up to date and reflect our current position, and
 - in the unlikely event of a data breach, (see 10 below on 'Personal data breaches') we will ensure that records are kept regarding the breach and the action we took in response to it.

10. Personal data breaches

- Personal data breaches can include:
 - access to the data we hold by an unauthorised 3rd party
 - deliberate or accidental action (or inaction) by a controller or processor
 - sending personal data to an incorrect recipient
 - computing devices containing personal data being lost or stolen
 - alteration of personal data without permission; and
 - loss of availability of personal data.
- The school needs to ensure that there are robust systems in place to detect, investigate and report any breaches of personal data.
- The UK GDPR makes it clear that when a security incident takes place, we are required, as a matter of urgency, to establish whether a personal data breach has occurred and, if so, promptly take steps to address it. Some data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job whilst other breaches can significantly affect individuals whose personal data has been compromised. This needs to be assessed on a case by case basis.
- Under the UK GDPR we are required to report a personal data breach to the ICO within 72 hours, when it is felt that as a result of that breach there is likelihood of a risk to peoples' rights and freedoms. A breach can have a range of adverse effects on individuals which might include emotional distress and/or physical and material damage. Where it is not felt that this risk is likely, it is not necessary to report the breach, but we will still document the breach and justify the decisions that have been taken, together with any subsequent action.



- Where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms we will inform those individuals without undue delay.
- When reporting a breach, we are required to provide the ICO with the following information:
 - a description of the nature of the personal data and, where possible, the categories and number of individuals concerned together with the category and number of personal data records concerned
 - the name and contact details of our Data Protection Officer
 - a description of the likely consequences of the personal data breach; and
 - a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.
- See Appendix 8 for more detailed information on the process of reporting data breaches as well as from the [ICO's website](#).
- We will keep records of any data breach, whether or not we are required to inform the ICO

11. Securing and handling data held by the school

- All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them. This will be the responsibility of the Head Teacher.
- All staff understand that they must use the school's ICT systems in a responsible way to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users.
- All staff will follow the procedures laid out in their staff code of conduct regarding both secure data handling and use of the internet.
- If a member of staff believes that the data on any device is breached they must report it to a member of the SMT without delay.
- All personal or commercially sensitive data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. safe / fire safe / remote backup. This includes data held on fixed computers, laptops and memory sticks.
- Staff should **not** remove or copy sensitive data from the organisation or authorised premises unless the media is:
 - encrypted,
 - is transported securely
 - will be stored in a secure location.
- This type of data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc).
- 'School to school'³ and internal exchange of data should be done via email or paper, providing a link to the location of data on the secure server. Alternatively, data transfer should be through a secure encrypted email system e.g. S2S, SecureNet Plus, common transfer files and school census data. If this is not available then the file must, as a minimum precaution, be password protected before sending via email. The password must be sent by other means and on no account included in the same email. A record of the email should be kept, to identify when and to whom the email was sent, (e.g. by copying and pasting the email into a Word document). Never put personal information such as pupils' names in the subject line of any email.
- When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by a technician using a recognised tool, e.g. McAfee Shredder.
- The school's wireless network (WiFi) will be secure at all times

³ [School to school service: how to transfer information](#) (DfE March 2014)



- The school will identify which members of staff are responsible for data protection. The school will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc. know what data is held, who has access to it, how it is retained and disposed of. This is shared with all staff concerned within the school.
- Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. **This information must not be stored on a personal (home) computer.**
- Members of staff (e.g. SMT members) who are given full, unrestricted access to an organisation's management information system should be aware that higher grades of sensitive data is accessible. **This information must not be stored on a personal (home) computer.**
- The school will keep necessary pupil and staff information in accordance with the guidance from the Department of Education and as stipulated in the school's own audit.
- When no longer required, the school should securely delete commercially sensitive or personal data as outlined in its audit.
- **Sharing and/or receiving personal data between the UK and third countries (countries outside the UK):**
- In the unlikely event that we are required to share data with third countries, we will follow [the procedures as outlined by the ICO](#).
- We have identified what data, if any, we receive from third countries and are aware who the data controller and processors of that data are and where the data is stored.
- We understand that we are responsible for carry out our own risk assessment and that we are complying effectively with UK GDPR

12. **Freedom of Information**

The school understands its obligations under the Freedom of Information Act 2000 and the procedures and supporting documents which explain the process can be found in Appendix 10.

13. **Policy review**

- This policy will be reviewed every 2 years or earlier in the event of any changes to legislation.