



School Privacy Notice

May 2018

Contents

Page	Section
3	Introduction
4	What Personal Information Do We Collect?
5	Why Do We Collect Personal Information?
7	Who Processes Your Personal Information?
8	How Do We Use Personal Information?
10	How Long Is Personal Information Stored For?
11	Sharing of my Personal Information
12	The National Pupil Database (NPD)
13	What Are Your Rights?
14	Requests for Information
15	Ensuring Our Data is Up-To-Date
16	Privacy Notice for the School Workforce
19	Appendix - Digital Personal Information and Data
21	Appendix - Paper-Based Personal Information and Data

1.0 - Introduction

This Privacy Notice is to help parents understand the following:

- How and why we collect your child's personal information.
- What we do with that information.
- The decisions that you can make about your child's information.

We are giving you this notice because you are able to exercise your child's data protection rights on their behalf. When your child is older (usually when they reach the age of 12) they will be considered mature enough to exercise their own data protection rights.

If you have any questions about this notice please talk to the Headteacher.

A separate Privacy Notice for the school workforce may be found on page 15.

1.1 - How We Define 'Personal Data'

Personal information is information that the school holds about your child and which identifies your child.

This includes information such as their date of birth and address as well as things like exam results, medical details and behaviour records. The school may also record your child's religion, ethnic group and nationality.

CCTV, photos and video recordings of your child are also classed as personal information.

2.0 - What Personal Information Do We Collect?

The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses.
- Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility.
- Attendance information – e.g. number of absences and absence reasons.
- Assessment information – e.g. National Curriculum assessment results.
- Relevant medical information.
- Information relating to Special Educational Needs and Disability (SEND).
- Behavioral information – e.g. number of temporary exclusions.

Please note, photos and videos of our children also constitute as personal data.

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

3.0 - Why Do We Collect Personal Information?

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

Heamoor School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, the Local Authority and/or the Department for Education.

We collect and use personal information in order to meet **legal obligations** and **legitimate, vital and public interests** (see below) as set out in the General Data Protection Regulations (GDPR) and UK law, including those in relation to the following:

- Article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulations (GDPR).
- Section 537A of the Education Act 1996.
- Section 83 of The Children's Act 1989.
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

3.1 - Collecting and Using Personal Information for Legitimate Interests

We believe that the processing of personal information is necessary for legitimate interests except where the processing is unfair to your child. The school relies on legitimate interests for most of the ways in which it uses your child's information. Specifically, the school has a legitimate interest in:

- Providing your child with an education, to support their learning and to monitor and report their progress.
- Safeguarding and promoting your child's welfare and the welfare of other children.
- Promoting the objects and interests of the school. This includes fundraising e.g. if we want to raise money to build new resources etc.
- Facilitating the efficient operation and quality of service of the school.
- Ensuring that all relevant legal obligations of the school regarding data sharing are complied with.

In addition, your child's personal information may be processed for the legitimate interests of others. For example, we may use information about your child when investigating a complaint made by another pupil.

If you object to us using your child's information where we are relying on our legitimate interests as explained above please speak to the Headteacher.

3.2 - Collecting and Using Personal Information for Legal Obligations

Where the school needs to use your child's information in order to comply with a legal obligation, for example to report a concern about your child's wellbeing to Children's Services. We may also have to disclose your information to third parties such as the Courts, the Local Authority or the police where legally obliged to do so.

3.3 - Collecting and Using Personal Information for Vital Interests

For example, to prevent someone from being seriously harmed or killed.

3.4 - Collecting and Using Personal Information for Public Interest

The school considers that it is acting in the public interest when providing education.

3.5 - Special Categories of Personal Information

The school must also comply with an additional condition where it processes special categories of personal information. These special categories include:

- Personal information revealing racial or ethnic origin.
- Religious beliefs.
- Health information.

We collect and use special categories of personal information in order to meet **vital interests, substantial public interests, legal claims and medical purposes** (see below) set out in the General Data Protection Regulations (GDPR) and UK law.

3.6 - Collecting and Using Special Categories of Personal Information for Substantial Public Interest

The processing of special categories of personal information is necessary for reasons of substantial public interest.

3.7 - Collecting and Using Special Categories of Personal Information for Vital Interests

To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

3.8 - Collecting and Using Special Categories of Personal Information for Legal Claims

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

3.9 - Collecting and Using Special Categories of Personal Information for Medical Purposes

This includes medical treatment and the management of healthcare services.

We may ask for your consent to use your child's information in certain ways. If we ask for your consent to use your child's personal information you have the right to withdrawn this consent at any time. Any use of your child's information before you withdraw your consent remains valid. Please speak to the Headteacher if you would like to withdraw any consent given.

4.0 - Who Processes Your Personal Information?

Heamoor School is the **data controller** of the personal information you provide to us.

This means the school determines the purposes for which, and the manner in which, any personal data relating to our pupils and their families is to be processed. **Carol Nicholls** (School administrator) acts as a representative for the school with regard to its data controller responsibilities and data policies; he can be contacted on:

- 01736 364868
- secretary@heamoor.cornwall.sch.uk

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data.

Where the school outsources data to a third party processor, the same data protection standards that Heamoor School upholds are imposed on the third party in acting as one of our data processors.

Lesley Osborne is the school's **Data Protection Officer**. This role is to oversee and monitor the school's data protection procedures, and to ensure we are compliant with the GDPR. The Data Protection Officer can be contacted on:

- 01736 364868
- dpo@heamoor.cornwall.sch.uk

The role of the Data Protection Officer is to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.0 - How Do We Use Personal Information?

Below are some examples of the different ways in which we use personal information and where this personal information comes from. Please note that this list is not exhaustive.

Example 1	The admissions forms which you complete give us personal information about your child. We also get information from your child and their teachers. Your child's old school may also give us information about your child if we need this to teach and care for them.
Example 2	<p>Sometimes we get information from your child's doctor and other professionals where we need this to look after your child. We collect this information to help the school run properly, safely and to let others know what we do here. Here are some examples:</p> <ul style="list-style-type: none"> • We need to tell all appropriate members of staff if your child is allergic to something or might need extra help with some tasks. • We may need to share information about your child's health and wellbeing with the School Nurse or counsellor.
Example 3	We may use CCTV to make sure the school site is safe. CCTV is not used in private areas.
Example 4	We may need to report some of your child's information to the Government. For example, we may need to tell the Local Authority if we have any concerns about your child's welfare.
Example 5	We may need information about any court orders or criminal petitions which relate to your child. This is so that we can safeguard your child's and other children's welfare and wellbeing
Example 6	If your child is from another country we have to make sure that they have the right to study in the UK. We might have to provide their information to UK Visas and Immigration.
Example 7	Depending on where your child will go when they leave us we may need to provide their information to other schools. For example, we may share information about your child's assessment results and we may need to pass on information which they need to look after your child.
Example 8	We may need to share information with the police or our legal advisers if an incident occurs or to help with an inquiry. For example, if one of your child's classmates is injured at school or if there is a burglary.
Example 9	Occasionally we may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the school properly. We might need to share your child's information with them if this is relevant to their work.
Example 10	If your child have misbehaved in a serious way, and the police have become involved, we may need to use information about the action taken by the police.
Example 11	We may share some information with our insurance company to make sure that we have the insurance cover that we need.
Example 12	We may share your child's academic and (where fair) their behaviour records with you or their education guardian so you can support their schooling.
Example 13	We will monitor your child's use of email, the Internet and mobile electronic devices e.g. iPads. This is to check that your child is not putting themselves at risk of harm. If you would like more information about this you can read the Acceptable Use Policy or speak to your child's class teacher.

Example 14	We may use photographs or videos of your child for our web site and social media sites or prospectus to show prospective pupils what we do here and to advertise our school. We may continue to use these photographs and videos after your child has left.
Example 15	Sometimes we use photographs and videos for teaching purposes, for example, to record a drama lesson. If you have any concerns about us using photographs or videos of your child please speak to your child's class teacher.
Example 16	We publish our news, sports fixtures etc. on the school web site and newsletters and put articles and photographs in the local news to tell people about what we have
Example 17	<p>We sometimes use contractors to handle personal information on our behalf. The following are examples:</p> <ul style="list-style-type: none"> • IT consultants who might access information about your child when checking the security of our IT network. • We use third party "cloud computing" services to store some information rather than the information being stored on hard drives located in school. <p>If you have any concerns about the above, please speak to the Headteacher.</p>

The Headteacher can answer any questions, which you may have about how we use your child's personal information.

5.1 - Sending Information to Other Countries

We may send your child's information to countries which do not have the same level of protection for personal information as there is the UK. For example, we may:

- Store your child's information on cloud computer storage based overseas; or
- Communicate with you about your child by email when you are overseas (for example, when you are on holiday).

The European Commission has produced a list of countries which have adequate data protection rules. The list can be found here:

http://ec.europa.eu/justice/dataprotection/international-transfers/adequacy/index_en.htm

If the country that we are sending your information to is not on the list or, is not a country within the EEA (which means the European Union, Liechtenstein, Norway and Iceland) then, it may not have the same level of protection for personal information as there is the UK. We will provide you with details about the safeguards which we have in place outside of this privacy notice. If you have any questions about the safeguards that are in place please contact the Headteacher.

6.0 - How Long Is Personal Information Stored For?

We keep your child's personal information for as long as we need to in order to educate and look after them. We will keep certain information after your child has left the school, for example, so that we can investigate in the event of a complaint.

In exceptional circumstances, we may keep your child's information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under data protection law.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Type of information	Retention period or the criteria used to determine the retention period
Parent correspondence and financial details	Six years after pupil has left school
Parent correspondence details	Five years after completion of paperwork
Pupil acceptance details	Six years after pupil has left the School
Pupil records	Transferred securely to the next School/ any records retained Six years after pupil has left the School

Details of how personal information is stored and disposed of may be found in the Appendix.

7.0 - Sharing of my Personal Information

The school is required to share pupils' data with the Department for Education on a statutory basis. The National Pupil Database (NPD) is managed by the Department for Education and contains information about pupils in schools in England.

The Department for Education may share information about our pupils from the National Pupil Database with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The Department for Education has robust processes in place to ensure that the confidentiality of any data shared from the National Pupil Database is maintained.

Heamoor School will not share your personal information with any third parties without your consent, unless the law allows us to do so. The school routinely shares pupils' information with:

- Pupils' destinations upon leaving the school
- The Local Authority.
- The NHS.
- The Department for Education.

8.0 - The National Pupil Database (NPD)

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

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections; such as the school census early years census. Some of this information is then stored in the National Pupil Database. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

For more information about the personal pupil data we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the National Pupil Database, go to; <https://www.gov.uk/government/publications/national-pupildatabase-user-guide-and-supporting-information>.

The Department for Education may also share information about our pupils from the National Pupil Database with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

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

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

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

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

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

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

9.0 - What Are Your Rights?

From May 2018, you will be able to make various decisions about your child's information.

Some of these are new rights whilst others build on your child's existing rights.

Your child's rights are as follows:

- If information is **incorrect** you can ask us to correct it.
- You can ask **what** information we hold about your child and be provided with a copy. We will also give you extra information, such as why we use this information about your child, where it came from and what types of people and organisations we have sent it to.
- You can ask us to **delete** the information that we hold about your child in certain circumstances. For example, where we no longer need the information;
- You can ask us to send you, or another organisation, certain types of information about your child in a format that can be read by computer.
- Our use of information about your child may be **restricted** in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy.
- Object to your personal data being processed.
- Where the processing of your data is based on your **consent**, you have the right to withdraw this consent at any time.

The Headteacher can provide more information about your child's data protection rights if required.

If you have a concern or complaint about the way Heamoor School and/or the Department for Education is collecting or using your personal data, you have the right to raise a concern or lodge a complaint with the supervisory authority; the **Information Commissioner's Office (ICO)**. The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

10.0 - Subject Access Requests for Information

Under data protection legislation, parents and pupils have the right to submit a Subject Access (SAR) to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the School Office (Mrs C Nicholls) or the Headteacher (Mrs J Flynn).

10.1 - How We Will Respond to a Subject Access Request (SAR):

- On receiving a request, we will contact the individual via phone to confirm the request has been received and will be processed.
- We will also verify the identity of the person making a request using 'reasonable means' (typically two forms of identification and one official proof of address).
- On receipt of identification, in most cases we will provide the information within 30 days and free of charge. If the request is complex or numerous, we will inform the applicant within 30 days that we will comply within 90 days and we will explain why the extension is necessary.
- If the request is made electronically, we will provide the information in a commonly used electronic format.
- We acknowledge that the school holidays are counted in the response time; if we receive a request in the school holidays, we will still respond within the same time frame.

10.2 - 'Unfounded or excessive' requests

Usually an 'unfounded' or 'excessive' request means that the request is repetitive, or asks for further copies of the same information.

If the request is unfounded or excessive, we reserve the right to either:

- Charge a reasonable fee to comply, based on the administrative cost of providing the information.
- Refuse the request.

10.3 - Refusing a request

If we refuse a request, we will:

- Respond within 30 days and explain the reason(s) for refusing the request.
- Inform the individual of their rights to complain to the Information Commissioner's Office.

11.0 - Ensuring Our Data is Up-To-Date

The school will, on an annual basis, share individual Data Collection Sheets with you in order to ensure that our records are accurate and up-to-date. Our admin staff will then update the information within our school MIS

12.0 - Privacy Notice for the School Workforce

The categories of school workforce information that we collect, process, hold and share include:

- **Personal information** (including employee or teacher number, National Insurance number, address, telephone number(s), marital status, DoB).
- **Special categories of data** including characteristics information such as gender, next of kin details, ethnic group.
- **Contract information** (such as start dates, hours worked, post, roles and salary information).
- **Work absence information** (such as number of absences and reasons).
- **Qualifications** (and, where relevant, subjects taught).

12.1 - Why We Collect and Use This Information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed.
- Inform the development of recruitment and retention policies.
- Enable individuals to be paid.

12.2 - The Lawful Basis on Which We Process This Information

We process this information under the following sections of the following regulations:

- General Data Protection Regulations (GDPR) Article 6(1)(b) - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- General Data Protection Regulations (GDPR) Article 9(2)(b) - processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Education Act (1996) for the purposes of departmental census. See the following web site for more information:
<https://www.gov.uk/education/data-collection-and-censuses-for-schools>

12.3 - Collecting This Information

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

12.4 - Storing This Information

We hold school workforce data for as long as you are employed by the school. On leaving, certain data will be retained to provide adequate information for future job references, such as periods of employment, roles and responsibilities etc.

12.5 - Who We Share This Information With

We routinely share this information with:

- Our Local Authority.
- The Department for Education (DfE).

12.6 - Why We Share School Workforce Information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

- **Local Authority** - We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- **Department for Education (DfE)** - We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

12.7 - Data Collection Requirements

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

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to;

<https://www.gov.uk/education/data-collection-and-censuses-for-schools>

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

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

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

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

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

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department: <https://www.gov.uk/contact-dfe>

12.8 - Requesting Access to Your Personal Data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the School Office (Mrs C Nicholls) or Headteacher (Mrs J Flynn).

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

The process for responding to a Subject Access Request (SAR) from a member of staff is shown Section 10.1 on page 14 of this document.

12.9 - Further Information

If you would like to discuss anything in this privacy notice, please contact the Headteacher.

Appendix - Digital Personal Information and Data

1.1 - Storage and Means of Access to Digital Data stored on the School MIS

All personal information listed here that is digitally stored on the school's Management Information System (MIS) is located on the school network. Access to this system is controlled as follows:

- Physical access to the school's server is restricted to the Network Manager and Headteacher.
- Access to the school network itself is made using individual usernames and passwords for all members of staff.
- Access to the school's MIS on the school network is restricted to key members of staff only, using different usernames and passwords.
- The levels of access to the school's MIS are set depending on the level and type of data access needed by each member of staff. Staff only have access to that level of data needed to fulfil their role. Access to any other data that is deemed to be unnecessary is restricted.
- All general access to the school's MIS is made on the school network only. The school network and MIS is remotely accessible by the School Network Manager and School Secretary using an encrypted connection for administrative purposes only.

1.2 - Security of Digital Personal Data Whilst In Use or Being Accessed in School

All staff accessing digital personal data ensure that:

- They log onto the school network and MIS using their own username and password.
- Their network or MIS passwords are not given out or used by any other members of staff.
- Their PC is password-locked when away from their desks to prevent unauthorised access.
- Due care and diligence is given when accessing digital personal data to reduce the chance of any over-the-shoulder access by unauthorised staff, pupils and parents / carers.
- Privacy screen covers are used as required to help prevent access by unauthorised staff, pupil and parents.
- Any data containing personal information that is sent for printing is sent to a password locked print folder which is accessed and printed locally.
- Any redundant printed data is shredded.
- Any digital personal data that is taken away from the school premises is loaded onto school-issued and managed encrypted memory sticks. Access to this data is via a complex password and all data is destroyed if the password is entered incorrectly ten times.

1.3 - Security of Digital Personal Data Whilst Being Shared by Others

Any digital personal data that is shared with anyone outside of the school is conveyed using the Cornwall Council authorised encrypted email service (AnyComms+).

1.4 - Disposal of Digital Personal Data

The disposal of all digital personal data from the school's MIS is the responsibility of the School Secretary.

The disposal of all other digital personal data from the school's network and data backup system is the responsibility of the Network Manager. All redundant digital personal data and data that has reached the end of its retention period is physically deleted. All redundant hardware that at any time contained personal digital data is physically destroyed to prevent further access prior to recycling.

1.5 – Other Digitally Stored Personal data

Heamoor School utilises a range of network and cloud-based educational and administrative resources that include the personal data of both our children and staff.

A full data audit has been carried out on each of these resources to provide as-complete-a-picture as possible of our current personal data deployment. For each resource the following areas have been examined:

- **Scope** – which personal and special category data items are contained with this resource.
- **Sharing** – if any of this personal data flow from this resource to another.
- **Retention** – what is the data retention policy for this resource and how does it align with our school retention policy to fulfil our role as a school? Is this retention policy clear within our contract/data policy of the resource supplier?
- **Data Request** - how would we gather the data out of this resource in response to a data request?
- **Own Readiness** – who is the resource supplier, what is their level of GDPR compliance and can they demonstrate this?
- **Access** – which users in school have read, write, read and write or no access to personal data for this resource.
- **Security** – what security arrangements are in place for this resource and do they correspond with any recognised standards?

The full details of each resource is shown in the school's **Personal Data Ecosystem** document on the school website.

Appendix - Paper-Based Personal Information and Data

2.1 - Storage and Means of Access to Paper-Based Personal Data

All personal data listed here that is stored in a printed format is physically located within the school building in locked filing cabinets/cupboards. Access to printed personal data is strictly controlled by the School Secretary, School safeguarding team, Headteacher and Class Teachers.

2.2 - Security of paper-Based Personal Data Whilst In Use or Being Accessed in School

All staff accessing paper-based personal data ensure that:

- No data is left unattended where it can be accessed by unauthorised members of staff, pupils or parents / carers.
- All data is collected from storage as it is required and promptly returned after use.
- All filing cabinets/cupboards are relocked each time they are accessed.
- Any redundant printed data is shredded.
- No data is displayed on classroom walls.

2.3 - Security of Paper-Based Personal Data Whilst Being Shared by Others

Any paper-based personal data that is shared with anyone outside of the school is conveyed using an authorised registered postal service.

2.4 - Disposal of Printed Personal Data

The disposal of all printed personal data from is the responsibility of the School Secretary. All redundant printed personal data and data that has reached the end of its retention period is shredded.