Personal Data Handling and Protection Policy

May 2018

Adopted	May 2018
Review	May 2019

Contents

1.0 - Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, Governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2.0 - Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

3.0 - Definitions

Personal data - Any information relating to an identified, or identifiable, individual.

This may include the individual's: Name (including initials).

- Identification number.
- Location data.
- Online identifier, such as a username.

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data - Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes.
- Health – physical or mental.
- Sex life or sexual orientation.

Processing - Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

Processing can be automated or manual.

Data Subject - The identified or identifiable individual whose personal data is held or processed.

Data Controller - A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor - A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4.0 - Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a **data controller**.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5.0 - Roles and Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Role	Responsibilities
The Governing Body	The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.
Data Protection Officer	The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the Body their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is **Lesley Osborne** and is contactable via phone (01736 364868) and email (dpo@heamoor.cornwall.sch.uk).
Headteacher	The Headteacher acts as the representative of the data controller on a day-to-day basis.

All Staff	Staff are responsible for:
	• Collecting, storing and processing any personal data in accordance with this policy.
	• Informing the school of any changes to their personal data, such as a change of address.
	• Contacting the DPO in the following circumstances:
	  ○ With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
	  ○ If they have any concerns that this policy is not being followed.
	  ○ If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
	  ○ If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
	  ○ In the event of a data breach – to report to the DPO as soon as possible.
	  ○ Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
	  ○ If they need help with any contracts or sharing personal data with third parties.

6. 0 - Data Protection Principles

The GDPR is based on data protection principles that our school must comply with.

The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7.0 - Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect Someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For **special categories of personal data**, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8.0 - Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a '**Subject Access Request**' or 'SAR' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 - Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a Subject Access Request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 – How We Will Respond to a Subject Access Request

- 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.

9.3.1 - '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.

9.3.2 - 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.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a Subject Access Request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10.0 - Parental Requests to See the Educational Record of Their Child

As a Trust School we are voluntarily permitting parents, or those with parental responsibility, to see their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. Records will be supplied free-of-charge, however we reserve the right to make a minimal charge of 2p per sheet for any additional copies requested. To use this service, please refer to the procedure detailed in the school's Freedom of Information policy, which is available on the school web site.

11.0 - Biometric Recognition Systems

The school does not use or currently intend to use biometric data. If this should change in the future, information on any system(s) employed will be detailed here.

12.0 - CCTV

We do not currently use CCTV in any location around the school site. If this changes, we will adhere to the ICO's code of practice for the use of CCTV.

13.0 - Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written **consent** from parents/carers as part of the Admissions Form for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school web site or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Social Media policy and eSafety policy for more information on our use of photographs and videos.

14.0 - Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15.0 - Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the School Office.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our eSafety policy and Staff Acceptable Use policy).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16.0 - Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out-of-date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17.0 - Personal Data Breaches

The school will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school web site which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

18.0 - Training

All staff and Governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19.0 - Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed annually and shared with the full Governing Body.

20.0 - Links with Other Policies

This data protection policy is linked to our:

- Freedom of information Policy.
- eSafety Policy.
- School Privacy Notice.
- Acceptable Use Policy.

Appendix : Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost.
    - Stolen.
    - Destroyed.
    - Altered.
    - Disclosed or made available where it should not have been.
    - Made available to unauthorised people.
- The DPO will alert the Headteacher and the Chair of Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to '*negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress)*', including through:
    - Loss of control over their data.
    - Discrimination.
    - Identify theft or fraud.
    - Financial loss.
    - Damage to reputation.
    - Loss of confidentiality.
    - Any other significant economic or social disadvantage to the individual(s) concerned.
- If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the DPO's User Documents, which is username and password protected.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website **within 72 hours**. As required, the DPO will set out:
- As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned.
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause.
    - Effects.
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

  Records of all breaches will be stored in the DPO's User Documents, which is username and password protected.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Data Breach Type - Sensitive information being disclosed via email (including safeguarding records).

It is school policy to send all sensitive information using the AnyComms+ encrypted email service supplied by Cornwall Council. However, should this data be inadvertently sent to an unauthorized individual, the following procedure will be used:

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Network Manager to recall it.

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an Internet search to check that the information has not been made public; if it has, we will contact the publisher/web site owner or administrator to request that the information is removed from their web site and deleted.

Data Breach Type - Personal data is accidently published on the school web or social media platforms

For example details of pupil premium interventions for named children, photos of children who do not have parental consent etc.

Note - the Network Manager/Headteacher are responsible for uploading and managing all content on the school web site. They will endeavor to check that any data, information or photos passed to him for web site and social media publication is permitted and that consents have been granted, however the overall responsibility for this lies with the person requesting the publication in the first instance.

In the event of personal data being accidently published on the school web site or social media platforms:

- The member(s) of staff who originally identifies the personal data published in error must alert the Network Manager and the DPO as soon as they become aware of the error.
- The Network Manager will remove this data as soon as possible and alert the DPO.
- The DPO will carry out an Internet search to check that the information has not been made public; if it has, we will contact the publisher/web site owner or administrator to request that the information is removed from their web site and deleted.

Data Breach Type - a school laptop containing non-encrypted sensitive personal data is stolen or hacked.

- The member(s) of staff who originally identifies the personal data loss must alert the Network Manager and the DPO as soon as they become aware.
- The DPO will carry out an audit with the member of staff to determine:
    - The type of data at risk.
    - The level of security on the device (password, fingerprint, facial recognition etc.).
    - The likelihood that an unauthorized user could gain access.
- The DPO will carry out an Internet search to check that the information has not been made public; if it has, we will contact the publisher/web site owner or administrator to request that the information is removed from their web site and deleted.