Data Protection Policy V3.0

Data Protection Policy

For Schools and Academies

Based on information provided by the Information Commissioners Office (ICO) and The Key.

Data Protection Policy V3.0

Table of Contents

Policy Statement

During the course of normal school activities we receive, use and store personal information about our pupils, parents, suppliers and staff. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018, which incorporates the requirements of the EU General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal and non-personal data we collect or process.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the School's Data Protection Officer Helen Gannon/admin@ebm.services.co.uk.

Definitions

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Data Subject is the living individual who's information is being processed.

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special Categories of personal data (previously referred to as Sensitive personal data) includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Special categories of personal data can only be processed under strict conditions, including with the consent of the individual.

The Data Controller is the Organisation or individual that decides the purpose of the processing, and how it will be processed.

The Data Processor is an Organisation or individual (other than an employee of the Data Controller) who processes data **on behalf of** the Data Controller (i.e. under their instructions).

Personal Data Breach is any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Data Controller

The School is the Data Controller and are registered with the ICO, renewed annually or as otherwise legally required. To enable us to comply with all Legislative obligations to the Department for Educations (DFE) and others, we process personal data relating to parents, pupils, staff, governors, visitors and others.

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.

Governing Board

The governing board 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. Where required, they will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Helen Gannon and is contactable at admin@ebm.services.co.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
    - If there has been a data breach
    - 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

Data Protection Principles

We will ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Data Protection Policy V3.0

Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Notifying Individuals

When we collect personal data directly from an individual, we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c. The third parties with which we will share or disclose that personal data.
d. If we intend to transfer personal data to a non-EEA country or international organisation, and the appropriate and suitable safeguards in place.
e. How individuals can limit our use and disclosure of their personal data.
f. Information about the period that their information will be stored, including when subject to statutory retention guidelines, or the criteria used to determine that period.
g. Their right to request from us, as the controller, access to and rectification or erasure of personal data or restriction of processing.
h. Their right to object to processing and their right to data portability.
i. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j. The right to lodge a complaint with the Information Commissioners Office.
k. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If we receive personal data about an individual from other sources, we will provide the data subject with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Data Protection Policy V3.0

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, except that which we are obliged to retain under statutory retention guidelines.

Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed.
b. Request access to any data held about them by a data controller.
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority.
e. Data portability.
f. Object to processing including for direct marketing.
g. Not be subject to automated decision making including profiling in certain circumstances.

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. Where necessary we will seek consent prior to sharing.
- 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 may 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.

Subject Access Requests

Individuals have a right to make a 'subject access request' 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

Data Protection Policy V3.0

- 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, to a nominated representative within the school, who will in turn liaise with our DPO. They should include:

- Name of individual
- Contact information
- Details of the information requested

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.

For Primary Schools

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. 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.

All requests should be made, in writing to the school admin officer (Yeading@yeadinginf.co.uk)

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request, without charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

We will not disclose personal data via telephone. All enquiries must be made in writing, either via letter or email.

Where a request is made electronically, data will be provided electronically where possible.

Freedom of Information Requests

The Freedom of Information Act (FOI) 2000 gives people the right to access information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and

Data Protection Policy V3.0

- members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data. Please refer to Subject Access Requests above. Applicants (requesters) do not need to provide a reason for wanting the information. On the contrary, the school must justify refusing them information.

All requests for information should be treated equally, except under some circumstances relating to vexatious requests and personal data. Because all requesters are treated equally, the school may only disclose information under the Act if it would disclose it to anyone who asked. In other words, consider any any information released under the Act as if it were being released to the world at large.

The school are able to refuse FOI requests under certain circumstances:

- It would cost too much or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

In addition, the school is permitted to withhold certain information that may relate to government policy or where we consider that harm would be likely to arise from disclosure, for example disclosure would be likely to prejudice a criminal investigation.

All FOI requests should be forwarded to the school admin officer.

Any concerns over whether information should be disclosed, or if a request may be refused should be discussed with our Data Protection Officer.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Data Protection Policy V3.0

Security procedures include:

- Any strangers seen in entry-controlled areas should be challenged/reported. Ensure all visitor protocols (e.g. visitors without DBS clearance accompanied at all times) are adhered to.
- 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. All desks and cupboards should be kept locked where they hold personal data.
- 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
- Staff must ensure that individual monitors do not show confidential information to passers by, and that they log off from their PC when it is left unattended.
- Where personal information needs to be taken off site, staff will be held responsible for it's security; and will be held accountable for any loss or breach.
- Data processing should only use as much data as is required to successfully accomplish a given task.
- All files containing personal data only kept on Trust/school approved systems (e.g Sims). Staff/governors/Directors will have Trust email addressess, remote access is in place and no confidential files will be stored on personal computers/laptops/phones/memory sticks or any other personal device.. Attachments to emails will be password protected where there is sensitive personal data.
- We will not use memory sticks
- Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

Transferring Personal Data Outside of the EEA

We may transfer any personal data we hold to a country outside the European Economic Area ('EEA') or to an international organisation, provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on public interest grounds, or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Data Security Technologies

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. All Data Processors are subject to a formal written agreement and are asked to supply evidence that they have adequate organisational and technological measures in place to protect that data.

Data Protection Policy V3.0

Disposal

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will 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.

Record Retention

We will only retain data for as long as is necessary to complete processing. However, where we have a statutory obligation to retain data please refer to our Retention Guidelines Policy.

We use the Information Records Management Soiety (IRMS) Toolkit for Schools as reference. A copy of this is available to view at http://irms.org.uk/page/SchoolsToolkit

Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

Signed by Chair of Governors ..... **Date** 2/5/18

Review Date: May 2020