Edward Peake C of E (VC) Middle School
Federation Headteacher: Miss Z J Linington

Potton Road • Biggleswade • Bedfordshire • SG18 0EJ
Tel: 01767 314562 • Fax: 01767 314006
E-mail: info@edwardpeake.beds.sch.uk
Web: http://www.edwardpeake.beds.sch.uk

Data Protection Policy

adopted by the Full Governing Body of Edward Peake Cof E (VC) Middle School

Contents Page

1 Introduction

Our school is committed to protecting the rights and freedom of all individuals in relation to the processing of their personal data.

2 Scope of this policy

The school needs to comply with the Data Protection Act 2018 and EU General Data Protection Regulations. This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing personal and special category data.

This policy and the legislation apply to all personal data, both that held in paper files and electronically. So long as the processing of the data is carried out for school purposes, it applies regardless of where data is held.

'Processing' data is widely defined and includes obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

3 Data protection principles

Personal and special category data must be:

3.1 Processed lawfully

All personal and special category data must be processed lawfully, fairly and in a transparent manner in relation to individuals

3.2 Used for a specific purpose

The data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3.3 Be relevant to the purpose

The data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

3.4 Be accurate

Data should be 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

3.5 Kept no longer than necessary

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

3.6 Kept securely

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

4 Responsibilities of staff and contractors.

Staff and contractors must:

- Complete the Data Protection Act 2018 training as soon as they join the school. This is a mandatory requirement.
- Complete an annual refresher course as directed by their manager
- Ensure that they only ever process personal data in accordance with requirements of the Data Protection Act 2018
- Follow the 6 Principles highlighted above.
- Seek help and advice from the data protection officer (DPO) when required via info@edwardpeake.beds.sch.uk

5 Personal data in the public domain

Our school holds certain information about people in the public domain, for example the Headteachers name will be on the website. Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

6 Data security

Keeping personal data properly secure is vital in complying with the Data Protection Act. All staff and contractors are responsible for ensuring that any personal data we have access to is kept securely. We are also responsible for ensuring that personal data is not disclosed inappropriately (either orally or in writing or accidentally) to any unauthorised third party.

This includes, as a minimum:

- We should always keep passwords safe and never share them. Follow the guidance on creating safe passwords here: https://www.cyberaware.gov.uk/passwords
- Lock away any personal data kept in paper format in a lockable cabinet or pedestal. Do not leave documents on desks unattended at any time
- If it is necessary to take hard copy documents out of the school make sure that those documents are looked after at all times, this includes note books and files. Consider whether it is necessary to take files out of the school at all or if so, take them on an encrypted handheld device or laptop.
- If data has to go onto a disc or memory stick make sure that the device that used is encrypted and that the data is password protected.
- If we have access to these devices make sure that they are stored securely and locked away safely when not being used.

7 Sending personal data securely

We can send documents containing personal data securely using the following methods:

Requested by:	Method:
Hard copy	Documents should be hand delivered to the data subject wherever possible. Check ID and address for sending before handing over documents. Make sure that the documents are securely contained in a sealed envelope. If it not possible for the data subject to collect the documents themselves use the **special delivery service** and include the name of the data subject on the envelope to ensure that they sign for the documents. **Note**: Check you have the correct address before posting
Encrypted device	Where the data is especially sensitive consider saving the documents on a password protected, encrypted memory device rather than posting hard copies. The password can be sent to the data subject once they have received the device by post to ensure that only they have access.
Email	**This is the preferred method**. Scan a copy of the file and move it to a secure location on the school's network. Send the file by secure data transfer [currently Egress]. Ask the data subject to confirm receipt of the documents as soon as possible

8 Data subject rights

Data subjects have defined rights over the use of their data. These rights have been reinforced and extended by the Data Protection Act 2018.

These rights are:

Informed

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the Data Protection Act 2018.
- We must provide individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.
- We must provide privacy information to individuals at the point of collection of their personal data from them.
- If we obtain personal data from other sources, privacy information must provided be within a reasonable period of obtaining the data and no later than 28 calendar days

Access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- We have one month [or 20 working days] to respond to a request.
- We cannot charge a fee to deal with a request in most circumstances.

Rectification

- The Data Protection Act 2018 includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- We have one month [or 20 working days] to respond to a request.
- In certain circumstances the school can refuse a request for rectification. Seek help from the Head Teacher to refuse a request to rectify data

Erasure

- The Data Protection Act 2018 introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- We have one month [or 20 working days] to respond to a request.
- The right is not absolute and only applies in certain circumstances.

Restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, the school is permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- We have one month [or 20 working days] to respond to a request.

Data Portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- The right only applies to information an individual has provided to a controller.

Object

- The Data Protection Act 2018 gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies the school may be able to continue processing if it can be shown that there is a compelling reason for doing so.
- The school must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- We have one month [or 20 working days] to respond to an objection

Automated decision making and profiling

The Data Protection Act 2018 has provisions on:

1. Automated individual decision-making (making a decision solely by automated means without any human involvement); and

2. Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The Data Protection Act 2018 applies to all automated individual decision-making and profiling. The Act has additional rules to protect individuals if the school is carrying out solely automated decision-making that has legal or similarly significant effects on them.

We can only carry out this type of decision-making where the decision is:

- Necessary for the entry into or performance of a contract; or
- Authorised by Union or Member state law applicable to the controller; or
- Based on the individual's explicit consent.

If we are carrying out any of these activities, we must:

- Give individuals information about the processing;
- Introduce simple ways for them to request human intervention or challenge a decision;

Carry out regular checks to make sure that the school's systems are working as intended.

The above rights are conditional depending on the reason we hold the data and why we may need to retain it.

Where we have a legal obligation to collect and process data or we are collecting the data to carry out a public task, we cannot always agreed with any objection application to the processing of that data. We will consider all requests and explain the reason for the decision.

Similarly if an individual claims that there is an error in the recording of a child protection meeting or a behavioural incident, it is unlikely that these records will be amended because it is likely that the records contain the professional opinion of a social worker or other professional. Whilst the school would be unable to amend the original we would be able to place the individual's objections on file next to the original record so that their objections can be noted.

Were we rely on consent to process data about an individual we will be obliged in most cases to apply the above rights.

9 Prohibited activities

The following activities are strictly prohibited when processing personal and special category data:

- Sharing passwords to access data
- Sending personal data to a personal email address to work on at home
- Sending data to unauthorised personal. Always check that the recipients are authorised to view the information being sent
- Sending personal data in an insecure format
- Losing or misplacing personal and sensitive data
- Leaving personal data unprotected
- Accessing information about a pupil or member of staff where there is no legitimate reason for doing do
- Accessing personal data about an individual for personal use
- Disclosing personal data to a third person outside of the school without a lawful basis

It is a condition of employment in the case of staff and contractors that they abide by the law and the policies of the school. Any breach of this policy could be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the school and/or the individual being held liable in law.

10 Privacy by Design

Under the Data Protection Act 2018 the School has a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. In order to achieve this, staff is expected to complete Privacy Impact Assessments to help identify and minimise any data protection risks

11 Privacy impact assessments (PIA)

The school must do a PIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data on a large scale.
- Use new technologies.
- Carry out profiling on a large scale, including evaluation or scoring of individuals.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

We must consider completing a PIA when you identify:

- Automated decision-making with significant effects.
- Systematic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

12 International transfers

The Data Protection Act 2018 imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

We may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by a legally binding agreement between public authorities or bodies or the transfer is

- Necessary for important reasons of public interest;
- Necessary for the establishment, exercise or defence of legal claims;
- Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- Made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

13 Exemptions

Exemptions to the Data Protection Act 2018 can apply in a small number of areas and only where the restriction respects the essence of the individual's fundamental rights and freedoms and it is a necessary and proportionate measure in a democratic society to safeguard:

- National security;
- Defence;
- Public security;
- The prevention, investigation, detection or prosecution of criminal offences;
- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- Breaches of ethics in regulated professions;
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- The protection of the individual, or the rights and freedoms of others; or
- The enforcement of civil law matters

14 Conclusion

Compliance with the Data Protection Act 2018 is the responsibility of all members of staff and contractors. Any questions about this policy or any queries concerning data protection matters should be raised with the Head Teacher.

15 Definitions

Subject Access Request or SAR	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.
Freedom of Information Request or FOI.	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
Personal Data	Personal data means data which relate to a living individual who can be identified directly or indirectly from the data, particularly be reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Examples of personal data are the name and address of an individual; email and phone number; a Unique Pupil reference number or an NHS number

Special Category Data	Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Information relating to criminal activities or convictions is not special category data but must be treated with similar safeguards in place. Special category data includes: race or ethnic origin of the data subject their political opinions their religious beliefs or other beliefs of a similar nature whether they are a member of a trade union their physical or mental health or condition their sexual life sexual orientation Biometrics (where used for ID purposes) Genetics
Confidential Data	Data given in confidence or data which is confidential in nature and that is not in the public domain. Some confidential data will also be personal data and/or special category data and therefore come within the terms of this policy. Staff working in social care and in management roles will handle confidential data regularly and must be careful not to disclose this information incorrectly.
Data Controller	The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The School is the data controller of all personal data used and held by the school.
Data Processors	Organisations or individuals who process personal data on behalf of the data controller are known as data processors. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
Data Subject	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
Lawful Basis	The grounds specified by the Regulations which need to be satisfied for any data processing to be legal. One ground needs to exist for processing personal data. Where special category data is processed a second ground must also exist.
Relevant Professional	The practitioners who supply information held on Social Services records, and various other medical and educational records. A relevant professional will consider where disclosure is likely to cause serious physical or mental harm to the applicant or any third party.
Data Breach	A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal

	data transmitted, stored or otherwise processed. A data breach may occur by accidentally sending an email to the wrong person or leaving a file in a public place. Breaches which result in a high risk to the individual must be reported to the ICO within 72 hours.

Signed _____
Chair of Governors

Date approved _____May 2018_____

Review date _____May 2020_____