Samuel Lucas JMI School

Data protection policy and privacy notice

Contents

1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

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

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force on 25th May 2018.

Maintained schools

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed

Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Office Manager.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the headteacher, or the Office Manager in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Privacy / Fair processing Notice

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the school office.

8. Subject access requests

Under the Data Protection Act 1998, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

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

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. The table at the end of the policy summarises the charges that apply.

If a subject access request does not relate to the educational record, we will respond within 40 calendar days. The maximum charge that will apply is £10.00.

9. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

10. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), 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. Staff and pupils are reminded to change their passwords at regular intervals
- 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 for school-owned equipment

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

12. Training

Our 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 or the school's processes make it necessary.

13. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in 25th May 2018.

We will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

14. Monitoring arrangements

Office Manager is responsible for monitoring and reviewing this policy.

Office Manager checks that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the governing board.

15. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

Appendix A

Principle 1: processing personal data fairly and lawfully

Principle 1 states that personal data shall be processed fairly and lawfully.

What is 'personal data'?

The DPA defines ‘personal data’ as data relating to a living individual.

This living individual must be identifiable from the data, or from the data along with other information that the data holder has or is likely to have in the future.

The DPA adds that personal data:

... includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Information Commissioner's Office (ICO) explains that this principle means that you must:

Have legitimate grounds for collecting and using the data

Not use the data in ways that have unjustified adverse effects on the individuals concerned

Be transparent about how you intend to use the data

Give individuals appropriate privacy notices when collecting their personal data

Handle people’s personal data only in ways they would reasonably expect

Make sure you do not do anything unlawful with the data

The ICO provides more details on how to comply with this principle. It looks at what the ‘conditions for processing’ are, as well as what privacy notices should cover.

Principle 2: processing personal data for specified purposes

Principle 2 says that personal data shall be obtained only for one or more specified and lawful purposes.

According to the ICO, to comply with principle 2, you must:

You must be clear from the outset about why you are collecting data and what you are planning to do with it

Be clear from the outset about why you are collecting data and what you are planning to do with it

Comply with the DPA’s fair processing requirements (including the duty to give privacy notices to individuals when collecting their personal data)

Comply with what the DPA says about notifying the information commissioner

Make sure that, if you wish to use or disclose the data for any purpose other than the originally specified purpose, the new use or disclosure is fair

Principle 3: the amount of personal data you may hold

According to principle 3, personal data shall be adequate, relevant and not excessive.

This principle means that you should make sure the data you hold about an individual is:

Sufficient for the purpose you are holding it

Not more than you need for the purpose you are holding it

The ICO guidance considers what is meant by “adequate, relevant and not excessive”, and also looks at when an organisation might be holding too much or too little personal data.

What is 'sensitive personal data'?

According to the DPA, ‘sensitive personal data’ is personal data made up of information relating to the data subject’s:

Racial or ethnic origin

Political opinions

Religious beliefs or beliefs of a similar nature

Trade union membership

Physical or mental health or condition

Sexual life

Commission or alleged commission of an offence (and any proceedings related to this)

Principle 4: keeping personal data accurate and up to date

Principle 4 says that personal data shall be accurate and, where necessary, kept up to date.

The ICO explains that the DPA takes into account that it may not be feasible to completely ensure the accuracy of all personal data collected. However, you should take "reasonable steps" to do this.

What constitutes 'reasonable steps' will vary depending on circumstances and "the nature of the personal data and what it will be used for".

You should also:

Make sure that the source of personal data is clear

Carefully consider any challenges to the accuracy of information

Consider whether it is necessary to update the information

Principle 5: retaining personal data

Principle 5 states that personal data processed for a purpose shall not be kept longer than is necessary for that purpose.

There are no precise retention periods for personal data, but this principle means that you should:

Review the length of time you keep personal data

Consider the purpose you hold the data when deciding whether (and for how long) to keep it

Securely delete information that is no longer needed for the specific purpose

Update, archive or securely delete out-of-date information

Principle 6: the rights of individuals

Principle 6 says that personal data shall be processed in accordance with the rights of data subjects.

Principle 6 requires you to process personal data in accordance with the rights of the individuals whose data you are holding. Individuals have the right to:

Access copies of the information held about them

Object to processing that is likely to cause, or is causing, damage or distress

Prevent processing for direct marketing

Object to decisions being taken by automated means

Have inaccurate personal data corrected, deleted or destroyed (in certain circumstances)

Claim compensation for damages caused by any breaches of the DPA

Individuals ... have the right to be told whether any of their personal data is being processed

Individuals can exercise their right to access information held about them by making a subject access request. Individuals who make written subject access requests have the right to be:

Told whether any of their personal data is being processed

Given a description of the personal data, the reasons it is being processed, and whether it will be passed on to anyone else

Given a copy of the information comprising the data

Given details of the source of the data (where this is available)

If you receive a subject access request from an individual, you can charge him or her a fee to cover costs. There are maximum allowable fees depending on the information you hold.

Principle 7: information security

Principle 7 requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

Principles of the DPA: video from the ICO

The eight principles of the DPA are outlined in the following video from the ICO.

The DPA sets out certain security requirements for holding personal data. The ICO explains that you should:

Make sure your security fits the nature of the data you hold and the harm that could result from a security breach

Be clear about who has responsibility for ensuring security

Make sure you have the right physical and technical security (this should be backed up by robust policies and procedures and well-trained staff)

Be ready to respond to security breaches swiftly and effectively

Principle 8: sending personal data outside the EEA

Principle 8 says that personal data shall only be transferred to countries outside of the European Economic Area (EEA) if certain conditions are met.

It stipulates that personal data should not be transferred out of the EEA unless the receiving country "ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".