



Castle View Primary School

Headteacher: Miss Claire Bright

Keswick Road, Lancaster, LA1 3LE

Tel. 01524 67880

Castle View Primary School Information Governance (Data Protection) Policy

1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents, visitors and third parties is collected, stored and processed in accordance with the Data Protection Act (DPA) 1998, the General Data Protection Regulation (GDPR) and the new Data Protection Act (DPA) 2018, and with other relevant legislation.

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](#) 2018 and Data Protection Act 2018.

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. This includes written or verbal data, and imagery.
Sensitive personal data	Data such as: 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, verbally, manually or digitally
Data subject	The person whose personal data is held or processed, such as: <ul style="list-style-type: none"> • Pupils. • Parents and Guardians. • Governors. • Employees or their families. • Members of the public. • Business partners. • Local authorities or public bodies.
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
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

4. 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 School 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.

The role of Data Protection Officer is assigned to the School Office Manager, Mrs Helen Holden.

The role of DPO Link Governor is Mrs Gemma Wylie.

Further details are in the school's statement of roles and responsibilities.

5. 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 School Office Manager.

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

For more detail see the school's Roles and Responsibilities document.

6. 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, lawfully and in a transparent manner in relation to individuals; the lawful basis can be:
 - Consent of a data subject
 - Processing is necessary for the performance of a contract with the data subject
 - Processing is necessary for compliance with a legal obligation (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014)
 - Processing is necessary to protect the vital interests of the data subject or another person (e.g. life or death)
 - Processing is necessary for the performance of a task carried out in the public interest

- The lawful basis for sensitive personal data (racial, political, religious, trade union, genetic, health, sex life, criminal convictions or offences) is:
 - Explicit consent of the data subject
 - Processing is necessary for carrying out obligations under employment, social security or social protection law
 - Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
 - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent
 - Processing relates to personal data manifestly made public by the data subject
 - Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
 - Processing is necessary for reasons of substantial public interest
 - Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services
 - Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or

- ensuring high standards of healthcare and of medicinal products or medical devices
- o Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- 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
- Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Privacy/fair processing notice

Further details are in the school's Pupil Privacy Notice, Workforce Privacy Notice, and **Third Parties' Privacy Notice**.

8. Subject access requests

Under data protection legislation, parents and pupils have a right to request access to information the school holds about them. This is known as a subject access request.

To make a request for your personal information, or be given access to your child's educational record, contact The School Office Manager, c/o Castle View Primary **School's School Office**.

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

- The pupil's/ individual'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 will be responded to within 1 month. The school may charge if more than one copy of the response or records are requested.

Following the ICO's guidance, if the school refuses a request, it will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We will do this without undue delay and at the latest, within one month.

The school will follow the Information Commissioner's guidance ('Subject Access Code Of Conduct' and <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>) in response to all subject access requests.

You also have the following rights:

- Right to be informed via a privacy notice.
- Right of rectification to incorrect data within 1 month.
- Right to erasure unless there is a legal reason for processing their data.
- Right to restrict processing to the bare minimum.
- Right to data portability to receive their data in the format they request.
- Right to object to personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling.

The school will ensure that these rights will be exercised.

9. Parental requests to see the educational record

As advised by the ICO (<https://ico.org.uk/for-the-public/schools/pupils-info/>) 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

The school will securely store and process all data it holds, as detailed in our Risk Assessment.

Records will be stored and retained as detailed in the IRMS Information Management Toolkit for Schools.

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. Risk assessment

The school has undertaken, and will regularly review, a risk assessment of its activities and identify those which are at most risk of resulting in a data breach. The school has then put control measures in place to manage the risks.

When considering introducing new systems the school will undertake a privacy impact assessment by following the ICO's guidance: <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf> and <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>, and making use of their template.

14. Data Breach

The school will establish monitoring procedures to detect, report and investigate a personal data breach, and will record the outcome of this monitoring.

If a data breach is identified the school will follow the Information Commissioner's guidance: <https://ico.org.uk/for-organisations/report-a-breach/>

Following the identification of a breach, the school will record the incident in its Data Breach Record.

Following the identification of a breach the school will undertake a review of its information governance risk assessments, and take steps to prevent a further occurrence of that nature.

Following the identification of a breach the school will notify the affected data subjects.

In the event of a data breach being detected the school will report the breach to the ICO within 72 hours from the discovery of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

15. Monitoring arrangements

The DPO and DPO Link Governor are responsible for monitoring and reviewing this policy. The DPO and DPO Link Governor checks that the school complies with this policy by, among other things, reviewing school records at least annually.

This document will be reviewed when the General Data Protection Regulation comes into force, and then annually.

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

16. 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 May 2018.

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

17. Links with other policies

- Information Governance handbook appendices.
- The freedom of information publication scheme.
- The IRMS Information Management Toolkit for Schools.
- Safeguarding Policy.
- Staff Code Of Conduct.
- Staff disciplinary and grievance policies
- Complaints policy.
- Whistleblowing policy.
- Security Policy.
- Online safety policy, and responsible use guidance.

Prepared by: Helen Holden: June 2020

To be approved by governors: Summer 2020.

To be reviewed: Summer 2021.