Data Protection (DP) Framework for Schools

Castleton C of E Primary School

Last Reviewed	**June 2025**
Reviewed By (Name)	**J Jackson**
Job Role	**Headteacher**
Next Review Date	
Version produced Spring 2025	Amendments indicated in green text. Updated the word 'should' to **'will'**.

This framework will be reviewed annually and **sooner when** significant changes are made to the law.

Schools will hold a record of staff acknowledgement of all policies.

Contents of this Framework (related documents)

Contents of this document

Introducing our DP Framework

This framework comprises of a number of key documents; including our Data Protection policy and other associated policies and procedures, which together form Castleton C of E Primary School's commitment to protecting the data of its pupils, families, staff and volunteers.

Compliance with this framework is mandatory for all staff.

"Personal data" means **any** information where a living person is either identified or identifiable, from the information alone, or with other information – these are known as Data Subjects. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in Social Media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system, or intended to be filed).

"Special category data" is personal data that needs more protection because it is sensitive.

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data

"Data Subjects" include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

"Data Controller" means the school, alone or jointly with other Data Controllers, decides on why and how personal data is processed.

"Processing" means collecting, storing, using, sharing and disposing of data.

"Processors" are the external bodies who processes personal data on behalf of the controller.

"Staff" includes current or former; permanent employees, temporary staff, agency staff, consultants, governors, volunteers, and anyone else working for the school. We will also expect job applicants and contractors (and their staff) to comply with this policy.

"Data Protection Officer" (DPO) is a statutory role with responsibility for:

advising the school about data protection obligations,

dealing with breaches, including suspected breaches and identified risks

monitoring compliance with this policy.

Our Data Protection Officer is: *Education Data Hub | Derbyshire County Council | County Hall, Matlock, Derbyshire DE4 3AG | 01629 532888 dpforschools@derbyshire.gov.uk*

"Data Protection Lead" is Jayne Jackson and is the member of school staff nominated to manage communication with the DPO.

Responsibilities

All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches to our Data Protection Officer.

All leaders are responsible for ensuring their team sign to confirm they have read, understood and will comply with the documents in this framework, before carrying out tasks that involve handling personal data, including reporting any suspected breaches.

DP Legislation & Regulator

1. Relevant legislation includes, but is not limited to:
    - Section 3 of the European Union (Withdrawal) Act 2018 (incorporates General Data Protection Regulation (EU) 2016/679 into the law of England and Wales, Scotland and Northern Ireland, to be known as the UK GDPR)
    - General Data Protection Regulation (GDPR);
    - Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;
    - Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling.)
    - Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
    - Human Rights Act 1998
    - Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials.
    - Protection of Freedoms Act 2012
    - Data (Use and Access) Bill
2. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.
3. Breaches of data protection legislation can cause the risk of real harm to people whose data is handled in an unfair or unlawful way, as well as significant monetary penalties and damage to reputation.
4. Individual members of staff may be prosecuted for committing offences under Sections 170, 171 or 173 of the DPA 2018. These offences are: obtaining, disclosing, altering or retaining data without the consent of the Data Controller; purposefully identifying people from data that has been "de-identified"; and purposefully withholding data that a data subject has requested, and is entitled to receive.