



**Wood Ley Community
Primary School**

DATA PROTECTION POLICY

Policy Owner:	Headteacher
Date:	September 2026
Review Date:	September 2027
Approved by:	Full Governing Body

Data Protection Policy:

Contents

1. Aims
2. Legislation and Guidance
3. Definitions
4. The Data Controller
5. Data Protection Principles
6. Roles and Responsibilities
7. Personal Data Breaches
8. Privacy Notices
9. Subject Access Requests
10. Parental Requests to Access their Child's Educational Record
11. Storage of Records
12. Disposal of Records
13. Training
14. Compliance with UK GDPR
15. Monitoring Arrangements
16. Links with Other Policies

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 UK GDPR and the Data Protection Act 2018.

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

2. Legislation and Guidance

This policy complies with the requirements of:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Education (Pupil Information) (England) Regulations 2005
- Guidance published by the Information Commissioner's Office (ICO)
- Department for Education guidance relating to schools and data protection.

The school will review this policy regularly to ensure it reflects current legislation and guidance.

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

Special Category Personal Data	Personal data requiring additional protection under Article 9 UK GDPR, including: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data • health data • sex life or sexual orientation
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

Wood Ley Community Primary School is the Data Controller for the personal data it processes. The Governing Body has overall responsibility for ensuring that personal data is processed lawfully, fairly and securely in accordance with the UK GDPR and the Data Protection Act 2018.

The school has appointed a Data Protection Officer (DPO) through Schools' Choice. The DPO provides independent advice and oversight on data protection compliance, monitors the school's compliance with UK GDPR and acts as a point of contact with the Information Commissioner's Office (ICO). Contact details for the DPO are published in the school's Privacy Notices and on the school website.

Day-to-day coordination of the school's data protection arrangements, including the administration of Subject Access Requests, records management and GDPR compliance, is delegated to the **Senior Administration and Finance Officer, Mrs G Tierney**.

The school is registered with the Information Commissioner's Office (ICO) as a Data Controller and maintains its registration in accordance with statutory requirements.

5. Data Protection Principles

The school will process personal data in accordance with the data protection principles set out in Article 5 of the UK GDPR. These require that personal data is:

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality

Accountability

6. Roles and Responsibilities

The **Governing Body** is responsible for ensuring that the school complies with its statutory obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated legislation.

The **Headteacher** has overall operational responsibility for implementing this policy, ensuring appropriate data protection procedures are in place and promoting a culture of good information governance throughout the school.

The school's **Data Protection Officer (DPO)** is appointed through Schools Choice. The DPO provides independent advice and guidance on data protection matters, monitors the school's compliance with data protection legislation and acts as the point of contact with the Information Commissioner's Office (ICO).

The **Senior Administration and Finance Officer** coordinates the school's day-to-day data protection arrangements, including records management, Subject Access Requests, staff guidance and operational GDPR processes. They work closely with the Headteacher and the Data Protection Officer to support the school's compliance with data protection legislation.

All staff, governors, volunteers and contractors who process personal data on behalf of the school are responsible for:

- processing personal data lawfully, fairly and securely;
- following the school's data protection policies and procedures;
- maintaining the confidentiality of personal information;
- reporting any actual or suspected personal data breach immediately in accordance with Section 7 of this policy; and
- completing mandatory data protection training and applying good information governance practices in their day-to-day work.

7. Personal Data Breaches

The school takes all reasonable steps to prevent personal data breaches. A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff, governors, volunteers and contractors must report any actual or suspected personal data breach immediately to the Headteacher or Senior Administration and Finance Officer. The Headteacher will ensure that the school's Data Protection Officer (DPO) is consulted promptly where appropriate. Staff must not attempt to investigate a significant breach themselves or delay reporting while trying to resolve the matter.

The school will investigate all suspected personal data breaches promptly and take appropriate action to contain the breach, minimise any risk to individuals and prevent recurrence.

Where required under the UK GDPR:

- personal data breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours of the school becoming aware of the breach;
- affected individuals will be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms; and
- all personal data breaches, regardless of whether they are reportable to the ICO, will be recorded in the school's Data Breach Register.

8. Privacy Notices

The school has produced detailed Privacy Notices for both pupil data (including data relating to parents & carers) and the school workforce (including volunteers). These are available for viewing on the school website as well as being displayed within the school building.

Those wishing to join the school (both parents and staff) have the availability of our Privacy Notices made clear through references made in our application and admissions forms, plus our Home – School Agreement document. They are asked to sign their acknowledgement of this on these forms.

8.1 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:

- Personal information (such as name, unique pupil number and address)
- Parent / Carer information (such as name, address, telephone number, email)
- Characteristics (such as ethnicity, language, nationality and free school meal eligibility)
- Attendance information
- Academic and assessment information
- Medical or Special Needs information
- Behavioural Information

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.

8.2 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 member of staff wishing to access their personal data should submit a Subject Access Request in accordance with Section 9 of this policy.

9. Subject Access Requests

Individuals have the right to request access to their personal data by making a Subject Access Request (SAR).

The school will normally respond within one calendar month of receipt of a valid request. Where permitted by law, this may be extended by up to a further two months for complex requests, in which case the requester will be informed.

The school will not normally charge a fee for responding to a Subject Access Request. A reasonable fee may only be charged where a request is manifestly unfounded or excessive, or where additional copies of information are requested.

Information may be withheld or redacted where an exemption applies, including where disclosure would adversely affect the rights and freedoms of another individual.

Under the UK GDPR and the Data Protection Act 2018, 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 may be made verbally or in writing. Where appropriate, the school may ask the requester to clarify the information they are seeking to help identify the personal data requested. 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

10. Parental Requests to see their Child's Educational Record

Parents have a separate statutory right to access their child's educational record under the Education (Pupil Information) (England) Regulations 2005. The governing body will make the educational record available for inspection, free of charge, within 15 school days of receiving a written request. Where a parent requests a copy of the educational record, this will also be provided within 15 school days. The school may charge a fee for providing a copy, but any charge will not exceed the cost of supplying it.

Requests for educational records are considered separately from Subject Access Requests made under the UK GDPR.

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. When a parent or carer makes a Subject Access Request on behalf of a child, the school will consider whether the child is able to understand their information rights and the implications of the request. Where the child is considered competent to exercise their own rights, the school will normally seek the child's authority before disclosing their personal data to a parent or carer. Each request will be considered individually, taking account of the child's age, maturity and ability to understand the request.

11. Storage of Records

The school takes appropriate technical and organisational measures to ensure that personal data is stored securely and protected against unauthorised access, loss, misuse or disclosure.

- Paper-based records and portable electronic devices, such as laptops and external hard drives containing personal information, are kept securely when not in use.
- Confidential paper records must not be left unattended on desks, in shared areas or displayed where they may be accessed by unauthorised individuals.
- Where confidential personal information is taken off site in paper form, staff must sign it in and out through the school office where appropriate. This does not include routine academic assessments or exercise books.
- Where personal information is taken off site in electronic form, it must only be stored on encrypted devices or accessed through approved secure school systems.
- Personal data stored electronically, including on approved cloud-based systems, must be protected through appropriate access controls, secure passwords and, where available, multi-factor authentication (MFA).
- School computers, laptops and other electronic devices containing personal data must be protected by secure user authentication and must not be left unattended while logged in.
- Encryption software is used to protect portable devices and removable media where appropriate.
- On-site backups are stored securely, and all off-site backups are encrypted before leaving the school site.
- Staff, governors and any authorised users who access school information using personal devices must comply with the school's information security requirements and apply the same standards of security expected for school-owned equipment.

12. 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.

13. 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.

14. Compliance with UK GDPR

The school processes personal data in accordance with the **UK GDPR, the Data Protection Act 2018** and associated legislation. The school will keep its data protection procedures under review to ensure continuing compliance with legislative and regulatory requirements.

15. Monitoring Arrangements

The Headteacher is responsible for ensuring compliance with this policy.

The effectiveness of this policy will be monitored through routine data protection practices, staff training, internal reviews and periodic audits of compliance.

The Governing Body will receive appropriate assurance that effective data protection arrangements remain in place.

This policy will be reviewed annually, or sooner where there are significant changes to legislation, regulatory guidance or the school's data processing arrangements.

16. Links with Other Policies

This policy should be read alongside the following school policies and procedures:

- Privacy Notices
- CCTV Policy
- Freedom of Information Publication Scheme
- Records Retention Schedule
- Online Safety Policy
- Acceptable Use Policy
- Complaints Policy
- Safeguarding and Child Protection Policy

The school's Privacy Notices are available on the school website and within the school. They explain how the school collects, uses, stores and shares personal information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.