

Data Protection Policy 2026 2027

Nothing is beyond our reach!

Policy Information

Item	Details
Policy Name	Data Protection Policy
Responsible Officer	Headteacher
Data Protection Officer (DPO)	Data Manager
Approved By	Governing Board
Date Approved	Autumn 2026
Review Date	Autumn 2027
Statutory / Non-Statutory	Statutory

Vision Statement

Nothing is beyond our reach!
Care and challenge engage and motivate us!
Praise reassures and supports us!
Successes are celebrated and built on!

At Norton Community Primary School we are committed to providing a caring, safe, inclusive and respectful environment where every child feels valued and able to achieve their full potential.

1. Purpose

Norton Community Primary School recognises the importance of protecting personal information and is committed to processing personal data lawfully, fairly and transparently.

The school collects, stores and processes personal information about pupils, parents, carers, staff, governors, volunteers, contractors and visitors in order to fulfil its educational, safeguarding and operational responsibilities.

This policy sets out how the school complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Department for Education Data Protection in Schools guidance
- Information Commissioner's Office (ICO) guidance

The school recognises that effective information governance forms an essential part of safeguarding and organisational accountability.

2. Scope

This policy applies to:

- All employees
- Governors
- Volunteers
- Contractors
- Agency workers
- Third-party service providers

The policy applies to all personal data regardless of format, including:

- Electronic records
- Emails
- Paper files
- Photographs
- CCTV footage
- Audio recordings

3. Definitions

Personal Data

Information relating to an identifiable living individual.

Examples include:

- Name
- Address
- Date of birth
- Unique pupil number
- Staff payroll details
- Attendance information

Special Category Data

Information requiring additional protection, including:

- Medical information
- Disability information
- Ethnicity
- Religious beliefs
- Biometric information

Processing

Any operation carried out on personal information, including:

- Collection
- Storage
- Recording
- Sharing
- Retrieval
- Deletion

4. Data Protection Principles

The school will adhere to the seven UK GDPR principles.

4.1 Lawfulness, Fairness and Transparency

Information will only be processed where there is a lawful basis.

4.2 Purpose Limitation

Information will only be used for specified and legitimate purposes.

4.3 Data Minimisation

Only information necessary for the intended purpose will be collected.

4.4 Accuracy

Reasonable steps will be taken to ensure information is accurate and up to date.

4.5 Storage Limitation

Data will not be retained longer than necessary.

4.6 Integrity and Confidentiality

Appropriate security measures will be implemented.

4.7 Accountability

The school must be able to demonstrate compliance with data protection legislation

5. Roles and Responsibilities

Governing Board

The Governing Board will:

- Ensure compliance with data protection legislation.
- Monitor information governance arrangements.
- Receive assurance regarding cyber security and data protection risks.
- Approve this policy and review it regularly.

Headteacher

The Headteacher has overall responsibility for compliance and will:

- Ensure implementation of this policy.
- Provide appropriate resources.
- Ensure staff training.

- Report significant risks to governors.

Data Manager

The Data Manager will:

- Coordinate day-to-day compliance activities.
- Maintain records of processing activities.
- Manage retention schedules.
- Support data breach management.

Data Protection Officer (DPO)

The DPO will:

- Provide advice and guidance.
- Monitor compliance.
- Support DPIAs.
- Liaise with the ICO where necessary.

Staff

All staff must:

- Follow this policy.
- Keep information secure.
- Report concerns immediately.
- Complete mandatory training.

6. Lawful Bases for Processing

The school relies upon one or more lawful bases:

- Public Task
- Legal Obligation
- Contract
- Vital Interests
- Consent
- Legitimate Interests (where appropriate)

Special category data will only be processed where an additional condition applies.

7. Privacy Notices

The school will publish and maintain privacy notices explaining:

- What information is collected
- Why it is collected
- The lawful basis for processing
- Who data may be shared with
- Retention periods

- Individual rights

Privacy notices will be available on the school website and upon request.

8. Data Sharing

The school may share information with:

- Department for Education
- North Yorkshire Council
- NHS and health professionals
- Safeguarding partners
- Examination bodies
- Educational software providers

Information will only be shared where lawful, necessary and proportionate.

9. Subject Access Requests (SARs)

Individuals have a right to access personal information held about them.

The school will respond within statutory timescales and will maintain procedures for:

- Identity verification
- Information gathering
- Review and redaction
- Secure disclosure

Further procedures are contained in Appendix A.

10. Photographs, Videos and Websites

The school may use photographs and videos for:

- Educational purposes
- Displays
- Newsletters
- School website
- Social media

Consent arrangements will be clearly communicated to parents.

The school will ensure all images are used appropriately and securely.

11. CCTV

Where CCTV is used, the school will ensure:

- Clear signage is displayed.
- Purpose is documented.
- Access is restricted.
- Retention periods are defined.
- Requests for footage are managed appropriately.

12. Information Security and Cyber Security

The school recognises cyber security as a safeguarding and governance issue.

Measures include:

- Password controls
- Multi-factor authentication where available
- Device encryption
- Anti-malware protection
- Regular updates and patching
- Secure backups
- User access controls
- Staff awareness training

The school will work with IT providers to maintain appropriate security standards.

13. Artificial Intelligence (AI)

Any use of AI tools must:

- Be authorised by school leadership.
- Comply with UK GDPR.
- Protect personal information.
- Not involve uploading sensitive data to unauthorised systems.

Staff should seek advice where uncertainty exists.

14. Data Protection Impact Assessments (DPIAs)

A DPIA will be completed where processing may present a high risk to individuals.

Examples include:

- New software systems
- Monitoring technologies
- Biometric systems
- Large-scale data sharing

The DPO will advise when DPIAs are required.

15. Records Retention and Disposal

The school will maintain a retention schedule.

Records will be:

- Stored securely
- Archived appropriately
- Destroyed confidentially when no longer required

See Appendix C.

16. Data Breaches

A data breach may include:

- Loss of information
- Inappropriate disclosure
- Cyber attack
- Ransomware incident
- Theft of equipment

All breaches must be reported immediately.

See Appendix B.

17. Complaints

Individuals may raise concerns through the school's complaints procedure.

They also have the right to complain to the Information Commissioner's Office.

18. Monitoring and Review

The Governing Board will review this policy annually or earlier if required due to:

- Legislative changes
- DfE guidance updates
- ICO recommendations
- Significant incidents

APPENDIX A

Subject Access Request Procedure

Stage 1 - Receipt

Requests should be sent to:

Data Protection Officer

Via the School Office

Requests may be made:

- In writing
- By email
- Verbally

Stage 2 - Verification

The school will verify identity before disclosure.

Acceptable evidence includes:

- Passport
- Driving licence
- Utility bill

Stage 3 - Information Gathering

Relevant information will be identified and reviewed.

Stage 4 - Redaction

Third-party information will be removed where necessary.

Stage 5 - Disclosure

Information will be supplied securely within statutory timescales.

APPENDIX B

Data Breach Reporting Form

Section	Details
Date and Time Discovered	
Reported By	
Location	
Description of Incident	
Information Involved	
Number of Individuals Affected	
Immediate Actions Taken	
Risk Assessment Completed By	
DPO Notified	Yes / No
ICO Notification Required	Yes / No
Lessons Learned	

APPENDIX C

Records Retention Schedule (Summary)

Record Type	Retention Period
Pupil Educational Record	Until pupil reaches age 25
Child Protection Records	DOB + 25 years
Personnel Files	6 years after employment ends
Payroll Records	6 years
Accident Records (Pupils)	DOB + 25 years
Accident Records (Staff)	7 years

Governing Board Minutes	Permanent
Admissions Records	Current year + 1 year
CCTV Footage	Normally 30 days unless required for investigation

(Refer to current ICO Information and Records Management Society guidance for detailed retention requirements.)

APPENDIX D

Privacy Notice Framework

Every school privacy notice should include:

Who We Are

School name and contact details.

What Information We Collect

- Pupil data
- Parent/carers data
- Staff data
- Visitor information

Why We Collect It

- Education provision
- Safeguarding
- Legal obligations
- Operational management

Who We Share It With

- DfE
- Local Authority
- NHS
- Safeguarding partners

How Long We Keep It

In accordance with the school's retention schedule.

Individual Rights

- Right of access
- Right to rectification
- Right to object
- Right to complain