Mickleton Primary School



Information Governance, Data Protection and Information Security Policy

Approved by:	FGB	**Date:**	September 2026
Next review due by:	September 2027		

1. Statement of Intent

Mickleton Primary School is committed to protecting personal information and ensuring that all information is handled lawfully, fairly, securely and transparently.

The school will comply with:

1 UK GDPR
2 Data Protection Act 2018
3 Freedom of Information Act 2000
4 Environmental Information Regulations 2004
5 Keeping Children Safe in Education
6 Relevant education and employment legislation
The school recognises that effective information governance supports safeguarding, educational provision, accountability and public confidence.

2. Scope

This policy applies to:

1 Staff
2 Governors
3 Volunteers
4 Contractors
5 Agency workers
6 Visitors handling school information
It applies to all information held by the school, including:

1 Paper records
2 Electronic records
3 Emails
4 Cloud systems
5 Photographs
6 CCTV
7 Mobile devices

3. Data Protection Principles

The school will process personal data in accordance with the UK GDPR principles:

1 Lawfulness, fairness and transparency
2 Purpose limitation
3 Data minimisation
4 Accuracy
5 Storage limitation
6 Integrity and confidentiality
7 Accountability
The school will be able to demonstrate compliance through policies, procedures, training, audits and records.

4. Lawful Processing

The school will identify a lawful basis before processing personal information.

The principal lawful bases used by the school are:

Lawful Basis	Typical Use
Public Task	Providing education and pupil support
Legal Obligation	Safeguarding, employment and statutory returns
Contract	Employment and service contracts
Vital Interests	Emergencies and protection of life
Consent	Photographs, publicity and optional activities

The school will only use consent where it can be freely given and withdrawn.

Where special category data is processed, an Article 9 condition will also be identified.

The school's Appropriate Policy Document is contained in Appendix Q.

5. Individual Rights

Individuals have the right to:

1 Be informed
2 Access their information
3 Rectify inaccurate information

4 Erase information in certain circumstances
5 Restrict processing
6 Object to processing
7 Data portability (where applicable)
8 Protection from solely automated decision-making
Requests should be directed to the school office or Data Protection Officer.

The school will normally respond within one calendar month.

6. Privacy Notices

The school maintains privacy notices for:

1 Pupils
2 Parents and carers
3 Staff
4 Governors
5 Volunteers
6 Contractors
Privacy notices explain:

1 What information is collected
2 Why it is collected
3 Who it is shared with
4 How long it is retained
5 Rights available to individuals
Current privacy notices are published on the school website.

7. Information Security

The school will implement appropriate technical and organisational measures to protect information.

These include:

Access Controls

- Role-based access
- Account management

- Regular access reviews

Device Security

- Secure devices
- Encryption where appropriate
- Prompt reporting of lost devices

Passwords and MFA

Users must:

- Keep passwords confidential
- Use strong passwords
- Enable multi-factor authentication where available

Email Security

Staff must:

- Check recipients carefully
- Use BCC where appropriate
- Avoid sharing excessive personal information

Remote Working

Staff accessing school information remotely must ensure information remains secure and inaccessible to unauthorised persons.

Artificial Intelligence

Personal, safeguarding, medical, SEND or personnel information must not be entered into AI systems unless approved and compliant with data protection requirements.

Physical Security

The school will maintain:

- Secure buildings
- Visitor controls
- Locked storage
- Confidential waste disposal

8. Information Sharing

The school may share information where:

- Required by law
- Necessary for safeguarding
- Necessary for educational provision
- Required to fulfil statutory duties
- Consent has been obtained where appropriate

Information sharing must be:

- Lawful
- Necessary
- Proportionate
- Secure

Safeguarding considerations will always take precedence where a child may be at risk of harm.

The school may share information with organisations including:

- Local Authorities
- Department for Education
- Social Care
- Health Services
- Police
- Other educational settings
- Approved service providers

9. Records Management

The school will:

- Maintain accurate records
- Store records securely
- Retain records only as long as necessary
- Dispose of records securely when retention periods expire

Each significant information system shall have an identified owner.

The school maintains:

- Information Asset Register
- Records Disposal Log
- Record of Processing Activities

Retention periods are detailed within Appendix R.

Retention will be suspended where records are subject to:

- Legal proceedings
- Safeguarding investigations
- Complaints
- Subject Access Requests
- Freedom of Information requests

10. Freedom of Information

The school complies with the Freedom of Information Act 2000.

The school will:

- Maintain a Publication Scheme
- Respond to requests within statutory timescales
- Provide advice and assistance where appropriate
- Apply exemptions lawfully

Requests must be made in writing.

The school will normally respond within 20 school days.

The school's:

- Publication Scheme is contained within Appendix O.
- Guide to Information is contained within Appendix P.

11. Data Breaches

A personal data breach includes any accidental or unlawful:

- Loss
- Destruction
- Alteration
- Disclosure
- Access

All actual or suspected breaches must be reported immediately to the Headteacher and Data Protection Officer.

The school will:

- Record incidents

- Investigate incidents
- Assess risk
- Notify the ICO where required
- Inform affected individuals where necessary

Where required, the ICO will be notified within 72 hours of becoming aware of a reportable breach.

The school maintains a Data Breach Register and Information Security Incident Log.

12. Data Protection Impact Assessments

The school will complete a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to individuals.

Examples include:

- New technologies
- AI systems
- New online platforms
- Monitoring technologies
- Processing involving vulnerable individuals

DPIAs will identify:

- Risks
- Mitigating actions
- Residual risks

Where appropriate, advice will be sought from the Data Protection Officer.

13. Training and Awareness

All staff will receive appropriate information governance training.

Training will include:

- Data protection
- Information security
- Safeguarding information sharing

- Cyber security awareness
- Data breach reporting

Training records will be maintained and monitored.

14. Roles and Responsibilities

Governing Board

Responsible for:

- Strategic oversight
- Policy approval
- Monitoring compliance

Headteacher

Responsible for:

- Day-to-day implementation
- Ensuring compliance
- Managing risks and incidents

Data Protection Officer

Responsible for:

- Independent advice
- Monitoring compliance
- Supporting incident management
- Liaison with the ICO

Staff

Responsible for:

- Following this policy
- Protecting information
- Reporting concerns and incidents
- Completing required training

Further details are provided in Appendix A.

15. Monitoring and Review

Compliance with this policy will be monitored through:

- Audits
- Information asset reviews
- Data breach monitoring
- FOI monitoring
- Subject rights monitoring
- Training records

This policy will be reviewed annually or sooner where:

- Legislation changes
- ICO guidance changes
- Significant incidents occur
- Operational requirements change

Associated Appendices

- Appendix A – Roles and Responsibilities
- Appendix B – Information Sharing Form
- Appendix C – Data Breach Reporting Form
- Appendix D – Breach Assessment Form
- Appendix E – Subject Access Request Form
- Appendix F – Data Rights Register
- Appendix G – FOI Request Form
- Appendix H – FOI Register
- Appendix I – Information Asset Register
- Appendix J – DPIA Screening Form
- Appendix K – Record of Processing Activities Template
- Appendix L – Disposal Log
- Appendix M – Training Record
- Appendix N – Security Incident Log
- Appendix O – Publication Scheme
- Appendix P – Guide to Information
- Appendix Q – Appropriate Policy Document
- Appendix R – Retention Schedule
- Appendix S – Staff Declaration

APPENDIX A

Roles and Responsibilities

Role	Responsibilities
Governing Board	Strategic oversight, policy approval and monitoring compliance
Headteacher	Day-to-day implementation and compliance
Data Protection Officer	Independent advice, monitoring and liaison with ICO
Designated Safeguarding Lead	Safeguarding information sharing and record management
Information Asset Owners	Security, access, retention and information quality
Staff	Compliance with policy and reporting concerns
Contractors	Compliance with contractual data protection obligations

APPENDIX B

Information Sharing Request Form

Organisation requesting information:

Contact name:

Purpose of request:

Information requested:

Lawful basis identified:

□ Public Task

□ Legal Obligation

□ Vital Interests

□ Consent

□ Other

Details:

Authorised by:

Date:

APPENDIX C

Data Breach Reporting Form

Reported by:

Date discovered:

Date incident occurred (if known):

Description of incident:

Type of data involved:

□ Pupil

□ Staff

□ Parent

□ Governor

□ Special Category

□ Safeguarding

□ Financial

Immediate action taken:

Reported to Headteacher:

□ Yes □ No

Reported to DPO:

□ Yes □ No

APPENDIX D

Personal Data Breach Assessment

Question	Yes/ No
Personal data involved?	
Special category data involved?	
Criminal offence data involved?	
Risk to individuals?	
Risk of identity fraud?	
Safeguarding implications?	
ICO notification required?	
Individuals need notifying?	

Decision and rationale:

Completed by:

APPENDIX E

Optional Subject Access Request Form

The school accepts Subject Access Requests made verbally, by email, letter or using this form.

Applicant Name:

Address:

Information Requested:

Proof of Identity Provided:

□ Passport

□ Driving Licence

□ Birth Certificate

□ Other

Date received:

APPENDIX F

Data Subject Rights Register

Ref	Request Type	Date Received	Due Date	Completed
	SAR			
	Rectification			
	Erasure			
	Restriction			
	Objection			

APPENDIX G

Freedom of Information Request Form

Name:

Email:

Information Requested:

Preferred Format:

□ Email

□ Paper

□ Inspection

Date:

APPENDIX H

Freedom of Information Register

Ref	Date Received	Subject	Outcome	Date Closed

APPENDIX I

Information Asset Register

Asset	Owner	Purpose	Location	Retention	Security Level

APPENDIX J

DPIA Screening Form

Project:

Description:

Will the project involve:

Question	Yes/ No
New technology?	
Special category data?	
Monitoring individuals?	
Vulnerable individuals?	
Large-scale processing?	
AI systems?	

DPIA Required?

□ Yes □ No

APPENDIX K

Record of Processing Activities (ROPA)

Activity	Purpose	Lawful Basis	Data Subjects	Retention
Admissions	Education	Public Task	Pupils	See Schedule
Employment	HR	Legal Obligation	Staff	See Schedule

APPENDIX L

Records Disposal Log

Date	Record Type	Method	Authorised By	Completed By

APPENDIX M

Data Protection Training Record

Name	Role	Date Completed	Refresher Due

APPENDIX N

Information Security Incident Log

Date	Incident	Risk Level	Action Taken	Closed

APPENDIX O

ICO Model Publication Scheme

The school has adopted the ICO Model Publication Scheme.

Information routinely published includes:

Who We Are

7 Governance structure
8 Staff structure
9 Contact details

Financial Information

7 Annual accounts
8 Budget information

Policies

8 Statutory policies
9 School procedures

Performance Information

8 Ofsted reports
9 School priorities

Services

9 Admissions

10 Curriculum
11 SEND provision

APPENDIX P

Guide to Information Available

Information normally available on request:

Category	Availability
School policies	Website
Governance information	Website
Curriculum information	Website
SEND information	Website
Financial summaries	Request
Complaints procedures	Website
Attendance information	Website

APPENDIX Q

Appropriate Policy Document

(Schedule 1 Data Protection Act 2018)

The school processes special category and criminal offence data where permitted under UK GDPR and the Data Protection Act 2018.

Special Category Data Processed

7 Health information
8 SEND information
9 Ethnicity information
10 Religion information
11 Safeguarding records

12 Occupational health records

Conditions Relied Upon

Activity	Article 6	Article 9
SEND provision	Public Task	9(2)(g)
Medical support	Public Task	9(2)(h)
Safeguarding	Legal Obligation	9(2)(g)
Occupational health	Legal Obligation	9(2)(b)

Safeguards

The school shall:

6 Restrict access.
7 Provide staff training.
8 Use secure systems.
9 Monitor compliance.
10 Review processing arrangements.

Retention

Information is retained in accordance with Appendix R.

Review

Reviewed annually by the Headteacher and DPO.

APPENDIX R

Personal Data Retention Schedule

Pupils

Record	Retention
Admissions	Admission + 1 year
Attendance	3 years
Behaviour	Date left + 1 year
Educational Record	Transfer to next school
SEND Records	DOB + 31 years
Child Protection	DOB + 25 years minimum
Medical Plans	Date left + 1 year

Staff

Record	Retention
Personnel File	Employment + 6 years
Recruitment (successful)	Employment + 6 years
Recruitment (unsuccessful)	6 months
DBS Certificate	Maximum 6 months
Payroll Records	6 years
Occupational Health	Employment + 6 years

Governance

Record	Retention
Signed Governing Board Minutes	Permanent
Complaints	6 years
Declarations of Interest	Term + 6 years

Finance

Record	Retention
Invoices	6 years

Accounts	6 years
Contracts (under seal)	12 years
Contracts	6 years

Information Governance

Record	Retention
SARs	3 years
FOI Requests	3 years
Data Breaches	6 years
DPIAs	Life of processing + 3 years

Disposal

Paper records shall be securely shredded.

Electronic records shall be securely deleted.

A disposal record shall be maintained.

APPENDIX S

Staff Acceptable Use and Information Security Declaration

I confirm that I have read and understood the school's:

- Information Governance, Data Protection and Information Security Policy
- Information Security requirements
- Acceptable Use requirements

I agree to:

- Protect confidential information.
- Maintain password security.
- Follow data protection requirements.
- Report incidents immediately.
- Use school systems responsibly.
- Comply with safeguarding requirements.

Name:

Role:

Signature:

Date: