



OUR MISSION: TO TRY OUR BEST, TO TELL THE TRUTH, TO LOOK AFTER EACH OTHER AND THE COMMUNITY

"Pupils' personal development, behaviour and welfare is OUTSTANDING" (Ofsted, 2019)

Data Protection Policy

2026

Approved by:	Mrs M.Norris – Headteacher	Date: September 2026
Chair of Governors	Mrs L.Glasper	
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

1. Aims
 2. Legislation and Guidance
 3. Definitions
 4. The Data Controller
 5. Roles and Responsibilities
 6. Data Protection Principles
 7. Collecting Personal Data
 8. Sharing Personal Data
 9. Subject Access Requests and Other Rights of Individuals
 10. Parental Requests to Access Educational Records
 11. CCTV
 12. Photographs and Videos
 13. Artificial Intelligence (AI)
 14. Data Protection by Design and Default
 15. Data Security and Storage of Records
 16. Retention and Disposal of Records
 17. Personal Data Breaches
 18. Training
 19. Monitoring Arrangements
 20. Links with Other Policies
 21. Appendix 1: Personal Data Breach Procedure
-

1. Aims

Stanley Crook Primary School aims to ensure that all personal data collected about pupils, parents and carers, staff, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with UK data protection legislation.

The school is committed to ensuring that personal information is handled lawfully, fairly and transparently whilst supporting the safeguarding and welfare of children.

This policy applies to all personal data, regardless of whether it is held electronically, digitally or in paper format.

2. Legislation and Guidance

This policy is based on:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Education (Pupil Information) (England) Regulations 2005
- Information Commissioner's Office (ICO) guidance
- Department for Education (DfE) guidance on data protection in schools
- DfE guidance on Generative Artificial Intelligence (AI) in education
- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- National Cyber Security Centre (NCSC) guidance

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
 - Online Safety Policy
 - Acceptable Use Policy
 - Staff Code of Conduct
 - Records Management and Retention Schedule
 - Freedom of Information Publication Scheme
-

3. Definitions

Personal Data

Any information relating to an identified or identifiable living individual.

Special Category Data

Personal data revealing:

- racial or ethnic origin
- religious or philosophical beliefs
- political opinions
- trade union membership
- health information
- biometric data
- genetic data
- sexual life or sexual orientation

Processing

Any operation performed on personal data including collecting, recording, storing, sharing, viewing, adapting or deleting.

Data Subject

The individual whose personal data is processed.

Data Controller

The organisation determining how and why personal data is processed.

Data Processor

An organisation processing personal data on behalf of the data controller.

Personal Data Breach

A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

Stanley Crook Primary School processes personal information relating to pupils, staff, governors, parents and carers, visitors and others and therefore acts as a Data Controller.

The school is registered with the Information Commissioner's Office (ICO) as required by law.

5. Roles and Responsibilities

5.1 Governing Board

The Governing Board has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The school has appointed an appropriately qualified and independent Data Protection Officer (DPO).

The DPO is responsible for:

- monitoring compliance with data protection legislation
- advising the school on data protection matters
- advising on Data Protection Impact Assessments (DPIAs)
- reporting data protection concerns to governors
- acting as the point of contact for the ICO and data subjects

Our DPO is Mrs M.Norris and can be contacted via stanleycrook@durham.sch.uk

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis and ensures that this policy is implemented effectively.

5.4 Designated Safeguarding Lead

The DSL will work closely with the DPO to ensure that safeguarding information is handled securely and shared appropriately.

5.5 All Staff

All staff are responsible for:

- following this policy
- keeping personal information secure
- reporting data breaches immediately
- seeking advice where unsure whether information may be shared
- completing mandatory training

6. Data Protection Principles

The school will ensure that personal data is:

- processed lawfully, fairly and transparently
- collected for specified and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date

- retained only for as long as necessary
- processed securely

The school will also comply with the principle of accountability and be able to demonstrate compliance with data protection legislation.

7. Collecting Personal Data

The school will only process personal data where there is a lawful basis under UK GDPR.

Where required, privacy notices will explain:

- what information is collected
- why it is collected
- how it will be used
- who it may be shared with
- how long it will be retained
- individuals' rights

The school will only collect information that is necessary for educational, safeguarding, employment or statutory purposes.

8. Sharing Personal Data

The school will only share personal data where there is a lawful basis to do so.

Information may be shared with:

- local authorities
- safeguarding partners
- health professionals
- social care
- the Department for Education
- examination and assessment bodies
- school service providers
- law enforcement agencies

Safeguarding Information Sharing

The school recognises that data protection legislation is not a barrier to safeguarding children.

Where concerns exist that a child may be suffering or is likely to suffer significant harm, information will be shared with appropriate agencies in accordance with:

- Keeping Children Safe in Education
- Working Together to Safeguard Children
- local safeguarding partnership procedures

Where appropriate, information may be shared without consent where seeking consent could place a child at greater risk or prejudice a safeguarding investigation.

The safety and welfare of the child will always be the paramount consideration.

9. Subject Access Requests and Other Rights

Individuals have rights under UK GDPR including:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to object
- rights relating to automated decision-making
- the right to data portability where applicable

The school will normally respond to Subject Access Requests within one calendar month.

10. Parental Requests to Access Educational Records

Parents with parental responsibility have the right to access their child's educational record in accordance with the Education (Pupil Information) Regulations.

Requests will normally be responded to within 15 school days.

This right may be restricted where disclosure could:

- place a child at risk of harm
 - adversely affect another individual
 - conflict with legal or safeguarding requirements
-

11. CCTV

The school operates CCTV systems for safeguarding, security and crime prevention purposes.

The school follows ICO CCTV guidance and ensures:

- signage is displayed
 - footage is stored securely
 - access is limited to authorised personnel
 - recordings are retained only as long as necessary
-

12. Photographs and Videos

The school may take photographs and videos for educational, communication and promotional purposes.

Appropriate parental consent will be obtained where required.

Photographs will be used in accordance with safeguarding considerations, parental preferences and any court orders or restrictions affecting individual pupils.

Photographs will not normally be accompanied by unnecessary personal information.

13. Artificial Intelligence (AI)

Stanley Crook Primary School recognises that Artificial Intelligence (AI), including generative AI tools, may support teaching, learning, administration and communication.

Any use of AI must:

- comply with UK GDPR and the Data Protection Act 2018

- comply with safeguarding requirements
- align with DfE guidance on AI in education
- be subject to meaningful human oversight
- not replace professional judgement

Staff must not enter personal, confidential, safeguarding or special category information into any AI platform unless:

- the platform has been approved by the school
- suitable contractual safeguards are in place
- any required Data Protection Impact Assessment has been completed

Staff remain responsible for all AI-generated content and must verify:

- accuracy
- appropriateness
- safeguarding implications
- bias and fairness

The school recognises that AI systems may generate inaccurate, biased or misleading information.

Any misuse of AI involving personal data or safeguarding information will be treated as a potential personal data breach.

14. Data Protection by Design and Default

The school will embed data protection into all processing activities.

This includes:

- maintaining privacy notices
- staff training
- privacy reviews
- compliance monitoring
- implementation of appropriate technical and organisational controls

The school will undertake a Data Protection Impact Assessment (DPIA) when introducing:

- new technologies
- AI systems
- surveillance systems

- online learning platforms
 - any processing likely to result in high risk to individuals
-

15. Data Security and Storage of Records

The school will protect personal data from unauthorised access, disclosure, alteration or destruction.

Measures include:

- role-based access controls
- secure storage of paper records
- encryption of portable devices
- secure transfer methods
- regular software updates
- cyber security controls
- staff awareness training
- secure backups

Personal devices used for school business must:

- be password protected
- use school-approved security measures
- use multi-factor authentication where available

Safeguarding records must not be permanently stored on personal devices.

Strong unique passwords must be used, and staff should not reuse passwords from personal systems.

Safeguarding Records

Child protection and safeguarding records will be maintained, stored, transferred and disposed of in accordance with statutory safeguarding guidance and the school's Safeguarding and Child Protection Policy.

Access will be restricted to authorised safeguarding personnel.

16. Retention and Disposal of Records

The school follows recognised retention guidance, including the Information and Records Management Society (IRMS) Schools Toolkit.

Personal information will be retained only for as long as necessary.

When records reach the end of their retention period they will be securely destroyed.

17. Personal Data Breaches

All staff must report suspected breaches immediately.

The school will:

- investigate suspected breaches
- assess risks
- record all breaches
- notify the ICO where required within 72 hours
- notify affected individuals where there is a high risk to rights and freedoms

Data breaches involving safeguarding information will be immediately referred to the Designated Safeguarding Lead and Data Protection Officer.

18. Training

All staff, governors and volunteers will receive appropriate data protection training as part of induction.

Training will include:

- GDPR requirements
 - safeguarding and information sharing
 - cyber security awareness
 - phishing awareness
 - AI and data protection
 - secure handling of safeguarding records
-

19. Monitoring Arrangements

The DPO and Headteacher are responsible for monitoring implementation of this policy.

The policy will be reviewed annually or sooner where required by:

- legislative changes
- ICO guidance
- DfE guidance
- safeguarding developments

20. Links with Other Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Staff Code of Conduct
- Acceptable Use Policy
- Freedom of Information Publication Scheme
- Records Management and Retention Schedule
- Behaviour Policy
- ICT and Cyber Security Procedures