



Hamer Community Primary School

Data Protection Policy

Approved by:	V Terry	Date: September 2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

1. Executive Summary	3
2. Introduction.....	3
3. Policy	4
4. Monitoring Compliance and Effectiveness of the Policy Document.....	9
5. Policy Review Date	9
6. Appendix.....	9
7. Glossary of Terms	9

1. Executive Summary

Information is a vital asset and resource for Hamer Community Primary School. It supports the education, safeguarding, welfare and development of pupils, the effective management of staff and services, and the governance and operation of the School.

This policy sets out the School's approach to:

Data Protection & Privacy

Data Quality

Information Security

Information Sharing

Records Management

Individual Rights and Requests

Data Protection by Design and Data Protection Impact Assessments

Children's information and digital technologies

Implementation of this policy will contribute significantly towards assuring pupils, parents/carers, staff, governors and other stakeholders that information is processed lawfully, fairly, transparently and securely. It supports the provision of high-quality education and services by promoting the effective and appropriate use of information.

The governing body has overall responsibility for ensuring that the School complies with relevant data protection obligations. The Headteacher acts as the representative of the governing body on a day-to-day basis. The School's Data Protection Officer (DPO) provides independent advice, information and monitoring in accordance with their statutory responsibilities.

2. Introduction

Hamer Community Primary School is committed to protecting the privacy and personal information of pupils, parents/carers, staff, governors, volunteers, visitors and other individuals whose information it processes. The School will handle information in accordance with applicable data protection legislation, statutory guidance and relevant codes of practice.

The principal legal framework is the UK General Data Protection Regulation (UK GDPR), supplemented and amended by the Data Protection Act 2018 and the Data (Use and Access) Act 2025 (DUAA). The School will also comply, where applicable, with the Freedom of Information Act 2000, the Privacy and Electronic Communications Regulations 2003, the Education (Pupil Information) (England) Regulations 2005, the Human Rights Act 1998, safeguarding legislation and the common law duty of confidentiality.

The DUAA amends the UK data protection framework rather than replacing the UK GDPR or Data Protection Act 2018. This policy will therefore be read as a single framework incorporating those legal requirements. The Information Commissioner's Office (ICO) continues to update guidance following the DUAA, and the School will review its procedures where relevant guidance changes.

The policy applies to information held on paper or electronically, including pupil and staff records, emails, photographs, CCTV, voice recordings, online learning records, assessment information, safeguarding records and information held in cloud-based systems.

Everyone managing or handling information on behalf of the School has a responsibility to comply with this policy. This includes:

- all employees of the School;
- governors and trustees where applicable;
- temporary, agency and supply staff;
- volunteers, students and trainees;
- contractors and other persons working on behalf of the School;
- suppliers and data processors where they handle School information.

The School recognises that managing information involves risks. This policy is intended to facilitate compliance, reduce those risks and provide a clear framework for the lawful, fair, transparent and secure handling of personal information.

The School will provide appropriate induction, refresher training and guidance. Staff must follow School procedures and seek advice from the DPO or a member of the senior leadership team where they are unsure how information should be handled.

3. Policy

3.1 Data Protection & Privacy

The School will process personal information in accordance with the principles of the UK GDPR and the Data Protection Act 2018, as amended by the DUAA. Personal information will be processed lawfully, fairly and transparently and only for specified, explicit and legitimate purposes.

The School will ensure that personal information is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- not retained for longer than necessary;
- processed securely using appropriate technical and organisational measures;
- processed in a manner for which the School can demonstrate accountability.

The School will identify and document an appropriate lawful basis for processing personal information. Depending on the circumstances, this may include public task, legal obligation, vital interests, contract, consent or legitimate interests where applicable. The School will not rely on consent simply because it is convenient; consent will only be used where it is an appropriate and freely given lawful basis.

Where special category information is processed, the School will identify both an Article 6 lawful basis and an appropriate Article 9 condition, together with any additional requirements under the Data Protection Act 2018. Criminal offence information will only be processed where the relevant legal conditions are satisfied.

The School will provide appropriate privacy information through its privacy notices and, where necessary, layered or topic-specific notices. Privacy information will explain what information is collected, why it is used, the relevant lawful basis, who it may be shared with, how long it is retained and the rights available to individuals.

The School will not normally use personal information for a new or incompatible purpose without first considering whether the proposed processing is lawful and compatible with the original purpose. Where required, the School will update its privacy information and complete a Data Protection Impact Assessment (DPIA).

The School recognises that children require particular protection in relation to their personal information. When processing or sharing children's information, the School will take account of their rights, needs and best interests and will apply a high standard of privacy by design and default.

3.2 Information Security

Information security is the practice of protecting information from unauthorised access or use, unlawful disclosure, accidental loss, alteration, destruction or other compromise.

The School will maintain appropriate technical and organisational measures to protect personal and other information. This includes controls relating to access, authentication, passwords, devices, networks, cloud services, email, physical records, backups, disposal and staff awareness.

Important information assets include paper records stored on or off site, computers, laptops, tablets, mobile phones, emails, data files, software, cloud platforms, CCTV, photographs, voice recordings and other recorded information.

Access to personal information will be limited to those who need it for legitimate School purposes. Staff must only access information necessary for their role and must not attempt to access information without appropriate authorisation.

School information must not be stored or transferred using personal accounts, unauthorised cloud storage, removable media or messaging applications unless expressly authorised by the School and appropriately secured.

Staff must take particular care when sending emails containing personal or sensitive information, including checking recipients and attachments before sending. Where appropriate, information must be encrypted, password protected or shared through an approved secure system.

School devices and accounts must be protected using appropriate passwords, multi-factor authentication where available, screen locking and other security measures required by the School.

Information assets and hardware that are no longer required will be disposed of securely in accordance with the School's retention and disposal arrangements.

All actual or suspected information security incidents or personal data breaches must be reported immediately in accordance with the School's Data Breach Procedure. Staff must not attempt to conceal, delete or investigate a suspected breach beyond the actions directed by the School.

3.3 Data Quality

Consistent, accurate, timely and comprehensive information is vital to support effective teaching, safeguarding, decision-making, funding, communication and the efficient operation of the School.

The School will take reasonable steps to ensure that personal information is accurate and, where necessary, kept up to date. Where an error is identified, the School will correct it without undue delay where appropriate.

Data quality is the responsibility of every member of staff who collects, enters, extracts, transfers or analyses information. Staff must take reasonable care when entering data, checking reports, transferring information or communicating personal details.

The School will maintain appropriate processes for correcting information and responding to requests from individuals to exercise their right to rectification.

3.4 Records Management

The School will ensure that records are created, maintained, stored, accessed and disposed of appropriately so that it can meet legal, regulatory, operational and safeguarding requirements.

School records will be accurate, reliable, secure and accessible to authorised persons. Records will be managed throughout their lifecycle from creation to eventual disposal.

The School will follow its Records Retention Schedule and will retain personal information only for as long as necessary for the relevant purpose, unless a longer period is required or permitted by law.

Records subject to an investigation, legal claim, safeguarding process, complaint, audit or other requirement must not be destroyed where the School has a legitimate reason or legal obligation to retain them.

Secure disposal will be used for both paper and electronic records. Staff must not place confidential or personal records in ordinary waste or recycle them through an insecure process.

3.5 Information Sharing

The School recognises that effective information sharing is essential to education, safeguarding, welfare and the delivery of services. At the same time, information must only be shared lawfully, fairly and securely.

Before sharing personal information, staff should consider:

why the information needs to be shared;

whether the sharing is necessary and proportionate;

the lawful basis for sharing;

whether special category or criminal offence conditions apply;

who needs the information;

what minimum information is required;

how the information will be transferred securely;

whether the sharing should be recorded;

whether any individual should be informed through the School's privacy information.

Consent is not automatically required for information sharing. Where another lawful basis applies, the School may share information without consent. Consent will be obtained where it is the appropriate lawful basis or where another legal or professional requirement makes it necessary.

Safeguarding remains a key consideration. The School may share information where necessary to protect a child or another person from harm and will follow safeguarding legislation and statutory guidance.

Where the School enters into a new or non-routine information sharing arrangement, particularly where the purpose, recipients, categories of data, technology or method of sharing changes, the School will assess the risks and put appropriate contractual or information-sharing arrangements in place.

The School will use Data Processing Agreements, Data Sharing Agreements or other contractual terms where appropriate. The School will undertake due diligence on suppliers and data processors and ensure that processors provide sufficient guarantees regarding security and compliance.

When considering the sharing of children's personal information, the School will take particular care and consider the best interests of the child. High standards of privacy and security will be the default.

3.6 Individual Rights and Requests

The School recognises the rights of individuals under data protection legislation. Depending on the circumstances, individuals may have rights including:

the right to be informed;

the right of access to personal information;

the right to rectification;

the right to erasure in applicable circumstances;

the right to restrict processing;

the right to data portability in applicable circumstances;

the right to object to processing;

rights relating to certain automated decision-making and profiling.

The School will maintain procedures for identifying, recording and responding to requests. A request does not need to use technical legal terminology. Staff who receive a request that may concern an individual's data protection rights must refer it promptly to the designated person/DPO rather than responding independently.

Subject Access Requests (SARs) will be handled in accordance with the UK GDPR and current ICO guidance. The School will carry out reasonable and proportionate searches and will consider applicable exemptions and the rights of other individuals.

A parent or person with parental responsibility may have separate rights to access a child's educational record under education regulations. These rights are distinct from a SAR and will be handled under the applicable education regulations.

For a maintained school in England, requests for access to a child's educational record are subject to the applicable education-record rules, including the relevant 15-school-day timescale. The School will distinguish these requests from UK GDPR subject access requests and will seek DPO advice where a request is unclear or overlaps both regimes.

The School will consider the age, maturity and understanding of a child when responding to requests for information about them. Parental responsibility does not automatically mean that a parent is entitled to all information about a child in every circumstance.

The School will maintain a clear route for data protection complaints. Complaints about the School's processing of personal information will be acknowledged within 30 days and responded to without undue delay, in accordance with the applicable statutory requirements. Individuals will also be informed of their right to complain to the ICO.

3.7 Data Protection by Design and Data Protection Impact Assessments

The School will consider data protection and privacy at the design stage of new projects, policies, systems, services and changes to existing practice.

A Data Protection Impact Assessment (DPIA) will be completed where required by law and will be considered for any processing that is likely to result in a high risk to individuals. DPIAs will be completed before high-risk processing begins and will be reviewed when the nature or risk of processing changes.

When procuring or introducing new digital platforms, apps, online learning systems, monitoring technologies or other services, the School will consider data protection, security, data minimisation, retention, international transfers, processor arrangements and children's privacy before implementation.

Where appropriate, the School will consult its DPO and the relevant LA or procurement/data protection advisers before introducing new processing.

3.8 Children's Information, Photographs, Video and Social Media

Children's information requires particular care. The School will use personal information only where there is a lawful and necessary reason and will apply appropriate safeguards.

Photographs and video recordings that identify pupils are personal data. The School will identify an appropriate lawful basis for their use and will follow its photography, privacy, safeguarding and social media arrangements.

The School will only publish identifiable pupil photographs, videos or other personal information through official channels in accordance with its privacy information and applicable permissions or other lawful basis.

Staff must not publish or share identifiable pupil information through personal social media accounts or unauthorised platforms.

The School's Social Media Policy sets out additional requirements for staff, parents/carers and other users concerning the publication and discussion of School-related information.

3.9 Digital Technologies, EdTech and Artificial Intelligence

The School recognises that digital technologies, educational technology and artificial intelligence (AI) can support teaching, learning, administration and professional practice but may also create data protection risks.

Staff must only use School-approved digital platforms, applications and AI tools for School work where the School has authorised their use.

Personal, confidential, safeguarding, special category or otherwise sensitive information must not be entered into a public or unapproved AI system. Staff must not upload pupil, parent/carers or staff information to an AI tool unless the School has confirmed that the tool is approved, the processing is lawful, appropriate safeguards are in place and any required data protection assessment has been completed.

Where AI or automated systems are used to support decisions affecting individuals, the School will consider applicable data protection requirements, transparency, human oversight, accuracy, fairness and the rights of affected individuals. AI must not replace appropriate professional judgement, safeguarding processes or statutory decision-making.

The School will consider children's rights and privacy when selecting and using EdTech products. Because pupils may not be able to choose whether to use a School-selected digital service, the School will seek to ensure that suppliers provide appropriate privacy, security and contractual safeguards.

Further guidance on acceptable use of AI and digital technologies may be provided through the School's Acceptable Use, Online Safety, Staff Code of Conduct or other relevant policies.

3.10 Data Breaches and Incident Management

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

Examples include sending information to the wrong recipient, losing a device containing personal data, sharing a pupil record with an unauthorised person, using an unauthorised system to store information, or accidentally making confidential information publicly accessible.

All staff must report actual or suspected breaches immediately to the School's designated data protection contact/DPO in accordance with the Data Breach Procedure. The fact that a breach was accidental does not remove the requirement to report it.

The School will assess reported incidents, take steps to contain and mitigate harm, document the incident and determine whether notification to the ICO or affected individuals is required. Where an ICO notification is required, the School will normally notify the ICO within the applicable statutory timescale.

The School will learn from incidents and may update procedures, training or technical controls following a breach.

3.11 Data Processors, Suppliers and Third Parties

Where a third party processes personal information on behalf of the School, the School will ensure that an appropriate written contract or other lawful arrangement is in place and that the processor provides sufficient guarantees regarding security and compliance.

The School will consider the processor's security measures, sub-processors, retention arrangements, deletion/return of data, confidentiality, data location and international transfers where relevant.

Staff must not independently sign up to or introduce an online service that requires pupil, parent/carers or staff personal information without following the School's procurement and data protection approval arrangements.

3.12 International Transfers

The School will consider whether personal information is transferred outside the UK, including where a cloud or technology provider stores or accesses information internationally.

Where an international transfer occurs, the School will ensure that the transfer is lawful and that appropriate safeguards or another permitted transfer mechanism are in place. Staff must refer proposed international transfers to the DPO or appropriate LA adviser.

3.13 Training and Responsibilities

The School will ensure that staff who handle personal information have access to appropriate data protection and information security training.

Managers are responsible for ensuring that staff understand the requirements relevant to their role. Training will include induction and periodic refresher activity, with additional training where staff have responsibilities involving safeguarding, HR, finance, administration, information systems or other sensitive information.

Staff are personally responsible for following this policy and reporting concerns promptly. Governors and other persons acting on behalf of the School must also protect information accessed through their role.

4. Monitoring Compliance and Effectiveness of the Policy Document

This policy will be subject to monitoring and compliance checks overseen by the DPO and School leadership. Monitoring may include reviews of information security incidents, data breaches, DPIAs, records management, data sharing, training, subject access requests, complaints and other relevant activity.

Information governance is viewed seriously by the School. Breaches of this policy or associated procedures will be investigated under the School's disciplinary arrangements, information security breach procedure or other appropriate process, depending on the circumstances.

Where a member of staff knowingly or recklessly misuses personal information, accesses information without authorisation, discloses information improperly or otherwise breaches data protection requirements, the School may take appropriate disciplinary or other action.

Where conduct may amount to a criminal offence, the School may take further action in accordance with legal advice and relevant procedures.

5. Policy Review Date

The DPO, Headteacher and School leadership will monitor this policy and review it at least annually. It will also be reviewed sooner where there are significant changes to legislation, ICO guidance, School systems, information processing, organisational arrangements or identified risks.

Next scheduled review: September 2027.

6. Appendix

6.1 Appendix A – Data Protection Principles

The School will apply the data protection principles contained in the UK GDPR, as amended by the Data (Use and Access) Act 2025. In summary, personal data must be:

processed lawfully, fairly and transparently in relation to the data subject;

collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes, subject to applicable legal provisions;

adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

accurate and, where necessary, kept up to date;

kept in a form that permits identification of data subjects for no longer than is necessary, subject to applicable legal requirements and permitted retention;

processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The School must also be able to demonstrate compliance with these requirements and will maintain appropriate technical and organisational measures and records to support accountability.

7. Glossary of Terms

Term	Meaning
------	---------

UK General Data Protection Regulation (UK GDPR)	The principal UK framework governing the processing and protection of personal data, as supplemented and amended by UK legislation.
Data Protection Act 2018	UK legislation that supplements the UK GDPR and contains additional rules and provisions relating to personal data.
Data (Use and Access) Act 2025	UK legislation that amends aspects of data protection and digital information law, including provisions affecting the UK GDPR and data protection complaints.
Personal data	Information relating to an identified or identifiable living individual.
Special category data	More sensitive personal data requiring additional protection, including information about health, racial or ethnic origin, religion, biometric data used for identification, and other categories specified by law.
Processing	Any operation performed on personal data, including collecting, recording, organising, storing, accessing, using, disclosing, transferring or deleting it.
Data Controller	The organisation or person that determines the purposes and means of processing personal data. The School is a data controller for information it determines how and why to process.
Data Processor	An organisation or person that processes personal data on behalf of a controller.
Data Protection Officer (DPO)	The person or service appointed to provide independent advice, information and monitoring concerning the School's data protection obligations and statutory DPO tasks.
Data Protection Impact Assessment (DPIA)	A process for identifying, assessing and reducing data protection risks associated with processing, particularly where processing is likely to result in a high risk to individuals.
Subject Access Request (SAR)	A request by or on behalf of an individual for access to their personal data under the right of access.
Data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Privacy notice	Information provided to individuals explaining how the School processes their personal information and the rights available to them.
Information Sharing Agreement	An agreement setting out the arrangements, responsibilities and safeguards for sharing information between organisations or services.
Data Processing Agreement	A contract or other legally binding arrangement setting out the requirements for a processor handling personal data on behalf of the School.

Records Retention Schedule	The School's schedule setting out how long different categories of records should be retained and when they should be securely disposed of.
ICO	The Information Commissioner's Office, the UK's independent regulator for information rights and data protection.
PECR	The Privacy and Electronic Communications Regulations 2003, which contain rules concerning electronic communications and related privacy matters.
Freedom of Information Act 2000	Legislation providing a general right of access to recorded information held by public authorities, subject to exemptions and other requirements.