



Data Protection Policy

Status of policy: Statutory

Frequency of review: Annually

Date of most recent review: Sept 2026

Date of next review: Sep 2027

Approved by FGB: 24th September 2026

1. Purpose and scope

This policy explains how Parkgate Primary School protects personal data and meets its responsibilities under UK data protection law. It applies to pupils, parents/carers, staff, governors, visitors, volunteers and other people whose information the school processes.

The school recognises that children need clear, age-appropriate information about how their personal data is used. The school will apply data protection in a proportionate way and will not collect, use or retain personal data simply because it might be useful.

2. Legal Framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Data (Use and Access) Act 2025 (DUAA)
- The Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE 'Keeping children safe in education'

1.2. This policy will also have regard to the following guidance:

- ICO 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE 'Data protection in schools'
- DfE 'The Data Use and Access Act 2025'
- ICO 'Data (Use and Access) Act 2025' guidance
- DfE 'Generative artificial intelligence (AI) in education'
- DfE 'Generative AI: product safety standards'

3. Data Protection Principles

Personal data will be processed lawfully, fairly and transparently; collected for specified purposes; limited to what is necessary; kept accurate; kept only as long as needed; and protected against unauthorised or unlawful processing, loss, destruction or damage. The school is accountable for demonstrating compliance.

Personal data includes information about an identified or identifiable living person. Special category data includes, for example, health, biometric, racial or ethnic origin, religion, and other categories requiring additional protection. Criminal offence data receives additional safeguards.

4. Accountability

The school is the data controller for the personal data for which it determines the purposes and means of processing. Governors and school leaders provide appropriate governance, resources and oversight. Staff and governors must follow school procedures, keep information secure, use only authorised systems, and report concerns promptly. The school will maintain its registration with the Information Commissioner's Office (ICO) where required.

The school maintains appropriate records of processing and applies data protection by design and by default. A Data Protection Impact Assessment (DPIA) will be completed where required, including where processing is likely to result in a high risk to individuals and where appropriate for new technology, substantial changes in processing, or systematic monitoring.

The school's Data Protection Officer (DPO) is:

Schools Data Protection Officer
Cheshire West and Chester Council,
4 Civic Way
Ellesmere Port
CH65 0BE
Email: schoolDPO@cheshirewestandchester.gov.uk

5. Lawful processing

Before processing personal data, the school identifies and documents the lawful basis that applies to the particular processing activity. Depending on the circumstances, this may include legal obligation, public task, contract, vital interests, legitimate interests where legally available, or consent.

For special category data, an additional Article 9 condition will be identified where required. Criminal offence data will be processed only where the applicable requirements of Article 10 UK GDPR and the Data Protection Act 2018 are met.

Consent is not the default lawful basis for routine school activities. Where consent is relied upon, it must be freely given, specific, informed and unambiguous, recorded, and capable of being withdrawn. For information society services offered directly to a child where consent is the lawful basis, the UK GDPR threshold is 13; where the child is under 13, consent must be

obtained from or authorised by a person with parental responsibility. The school will not use consent where another lawful basis is more appropriate.

6. Consent

Consent is not the default lawful basis for school activities. Where consent is used, it must be freely given, specific, informed and unambiguous, recorded, and capable of being withdrawn. For online services offered directly to a child on the basis of consent, the UK GDPR child-consent threshold is 13; below that age, parental responsibility holder consent is required where consent is the lawful basis. The school will not use consent where another lawful basis is more appropriate.

Where consent is used, the school will provide clear information about what is being consented to and will record the consent given.

Consent will be reviewed where circumstances change and will be capable of withdrawal. Withdrawal will be respected unless another lawful basis applies.

The school will not make routine access to education or services conditional on consent where consent is not genuinely voluntary or another lawful basis is available.

7. Privacy information and children

The school will make appropriate privacy notices freely available on its website and elsewhere as required. Privacy information will be clear, concise, accessible and, for children, age-appropriate. It will explain what personal data is collected, why it is used and the relevant lawful basis, who it may be shared with, retention periods or criteria, international transfers where relevant, individual rights, how to complain, and any relevant automated decision-making or profiling. Significant changes to processing or privacy information will be communicated appropriately.

Parents/carers will receive the school's privacy information and, where appropriate, information about how their child's data is used and shared. Parental access to information is subject to the child's rights, the child's maturity and understanding, and any safeguarding or legal considerations.

8. Individual rights and information requests

Individuals have rights under data protection law, including rights of access, rectification, erasure, restriction and objection and, where applicable, data portability. These rights are subject to statutory conditions and exemptions and do not automatically require deletion of records that the school has a legal obligation or other lawful reason to retain. The school will consider children's rights directly and will not assume that a parent/carer can exercise a child's rights in every circumstance.

Subject Access Requests (SARs), Freedom of Information requests and other information-rights requests will be handled promptly under the school's procedures and applicable

statutory timescales. The school will verify identity where necessary and consider safeguarding, confidentiality and third-party information before disclosure.

The school will provide a clear and accessible route for data-protection complaints. Complaints will be recorded, investigated and responded to without undue delay. The school will explain the outcome and, where appropriate, the individual's right to complain to the ICO.

9. Safeguarding and data sharing

Protecting children is a core responsibility. Personal data may be shared without consent where there is a lawful basis and the sharing is necessary, including for safeguarding, child protection, education, health, social care, legal or statutory purposes. Staff must share only information that is necessary and proportionate, with the appropriate person or organisation, using a secure method. Where appropriate, the school will document data-sharing arrangements and complete a DPIA before high-risk sharing.

The school will not allow data protection concerns to prevent necessary safeguarding information sharing. Staff should follow safeguarding and information-sharing procedures and seek advice from the DSL, DPO or other appropriate lead where needed.

10. Security and personal data breaches

Paper records containing personal data will be secured against unauthorised access. Digital information will use appropriate access controls, authentication, encryption or password protection, backups and device security. Staff must check recipients before sending information, use secure methods for confidential data, avoid unnecessary local or removable copies, and report mistakes immediately.

Staff must report suspected or actual personal data breaches immediately to the DPO/appointed reporting route. The school will assess, contain, investigate and document incidents. Where required, the ICO will be notified without undue delay and, where feasible, within 72 hours of becoming aware of a notifiable breach; affected individuals will be informed where the law requires. The school will take steps to prevent recurrence.

11. Records, retention and disposal

The school keeps personal data only for as long as necessary for the purpose and in accordance with its retention arrangements and relevant DfE/ICO guidance. Records will be securely destroyed or deleted when no longer required, subject to legal, safeguarding, audit or other legitimate retention requirements.

12. EdTech, cloud services and AI

Any EdTech, cloud or AI service that processes personal data must be assessed and approved before use. The school will consider the purpose and necessity of the processing, data minimisation, lawful basis, security, safeguarding, supplier/controller/processor roles, sub-processors, international transfers, retention and deletion, data-subject rights and

contractual protections. A DPIA will be completed where required. Contracts with processors will include the protections required by data protection law.

Pupil-facing technology will have appropriate filtering and monitoring, access controls and retention arrangements. Monitoring will be lawful, proportionate and transparent, and access to monitoring information will be restricted to authorised staff. Significant changes to processing or monitoring will be reassessed, including through a DPIA where required.

Staff and pupils must not enter personal, identifiable or sensitive information into public or unauthorised generative AI tools. Any approved AI service that processes personal data must have been formally assessed and approved, with an appropriate lawful basis, security and contractual safeguards. Approved AI use must comply with the school's Acceptable Use/Safe Use of AI arrangements, include appropriate human oversight, and any incident or suspected breach must be reported immediately.

The school will use only appropriately authorised digital services and will consider data protection before introducing new systems. Supplier arrangements will address security, confidentiality, data processing, sub-processors, international transfers, retention and deletion, data-subject rights and other required safeguards as appropriate.

Because pupils are children, the school will take particular care with online platforms, profiling, automated decision-making, monitoring and AI. The school will consider children's higher protection needs when designing and procuring processing. Where automated decision-making is used, the school will comply with applicable UK GDPR and Data Protection Act safeguards, including appropriate information, human involvement and routes to challenge decisions where required. Staff remain responsible for decisions affecting pupils and must check AI-generated outputs before relying on them.

13. Photography, video and CCTV

Identifiable photographs, videos and CCTV footage are personal data. The school will use them only where there is a clear lawful basis and in a necessary, proportionate and transparent way. CCTV will be signposted, access restricted and footage retained only as long as necessary. The school's current general CCTV retention period is up to 7 calendar days unless an incident, investigation or legal obligation requires longer retention. More detailed operational arrangements are set out in the CCTV Policy and relevant privacy information.

Parents and visitors may take photographs or videos at school events for personal or domestic use unless the school states otherwise. They must respect privacy and safeguarding and must not publish or otherwise share images containing another child where this would be inappropriate or contrary to the school's stated arrangements. Further operational requirements are set out in the school's relevant photography, video and CCTV arrangements.