Belmont Community Primary School

Data Protection Policy

2026/27

Approved by: Full Governing Body
Approval date: 1 October 2026
Review date: 1 October 2027

1. Purpose and scope

Belmont Community Primary School is committed to protecting the privacy and security of personal data. This policy explains how the school will collect, use, share, store and dispose of personal data and how it will meet its responsibilities under current UK data protection law.

The policy applies to personal data processed by the school about pupils, parents and carers, staff, governors, volunteers, visitors, contractors and other individuals. It applies to all staff and to external organisations or individuals who process personal data on the school's behalf.

The school will process personal data lawfully, fairly and transparently, with appropriate technical and organisational measures to protect it.

2. Legislation and guidance

This policy is based on the following legislation and current guidance, as applicable:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018 (DPA 2018), as amended.
- Data (Use and Access) Act 2025 (DUAA), including amendments that came into force during 2025 and 2026.
- Education (Pupil Information) (England) Regulations 2005, including provisions concerning access to education records.
- Freedom of Information Act 2000, where applicable.
- Department for Education guidance: Data protection in schools.
- Information Commissioner's Office (ICO) guidance and codes of practice.

Current DfE guidance: Data protection in schools

Current ICO guidance: ICO – UK GDPR guidance

The Data (Use and Access) Act 2025 does not replace the UK GDPR or Data Protection Act 2018; it amends them. The school will keep this policy and its associated procedures under review as legislation and official guidance develop.

3. Key definitions

Term	Definition
Personal data	Information relating to an identified or identifiable living individual.
Special category data	More sensitive personal data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health, sex life and sexual orientation.
Processing	Any operation performed on personal data, including collecting, recording, storing, using, sharing, altering or deleting it.
Data subject	The individual to whom personal data relates.
Data controller	The organisation that determines the purposes and means of processing personal data.
Data processor	A person or organisation that processes personal data on behalf of a controller.
Data Protection Officer (DPO)	The person responsible for advising on and monitoring compliance with data protection law and supporting the school in meeting its obligations.
Personal data breach	A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Privacy notice	Information explaining what personal data the school collects, why it is used, how long it is kept, who it may be shared with and the rights of individuals.

4. The data controller

Belmont Community Primary School is the data controller for the personal data it determines the purposes and means of processing. The school will maintain its registration with the Information Commissioner's Office (ICO) where required and will keep its data protection arrangements under review.

Where Lincolnshire County Council or another organisation is the controller for particular processing, the school will comply with the arrangements applicable to that processing.

5. Roles and responsibilities

5.1 Governing body

- Ensure that the school has appropriate data protection policies and procedures and that these are regularly reviewed.
- Provide appropriate oversight of data protection compliance and receive relevant assurance from the DPO or data protection lead.
- Ensure that sufficient resources and support are available to enable the school to meet its data protection responsibilities.

5.2 Data Protection Officer

- Monitor compliance with data protection law and this policy.
- Advise the school, governors and staff on data protection obligations.
- Provide advice on data protection impact assessments (DPIAs), data sharing and new processing activities.
- Support the management of information rights requests and personal data breaches.
- Cooperate with and act as the contact point for the ICO.

5.3 Headteacher and senior leaders

- Ensure this policy is implemented in day-to-day practice.
- Ensure staff receive appropriate training and guidance.
- Ensure that new or changed processing is considered through the school's data protection processes.

5.4 All staff and governors

- Only access and use personal data when necessary for their role.
- Keep personal data secure and follow school procedures.
- Report suspected data breaches immediately to the DPO or nominated data protection lead.
- Forward any information rights request to the DPO or nominated person immediately, including requests made verbally.
- Seek advice before introducing new processing, using a new system or sharing personal data where they are unsure of the lawful basis or appropriate safeguards.

6. Data protection principles

The school will comply with the seven UK GDPR data protection principles. Personal data must be:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification for no longer than necessary, subject to lawful retention requirements.
- Processed securely, using appropriate technical and organisational measures.
- Processed accountably: the school must be able to demonstrate compliance.

7. Collecting and processing personal data

7.1 Lawfulness, fairness and transparency

The school will identify and document an appropriate lawful basis for each processing activity. The lawful basis relates to the particular processing activity, not simply to the type of information being processed.

The six standard lawful bases under Article 6 UK GDPR are:

- Consent.
- Contract.
- Legal obligation.
- Vital interests.
- Public task or official authority.
- Legitimate interests, where the conditions for relying on this basis are met.

The DUAA has also introduced a separate recognised legitimate interest lawful basis for specified public-interest purposes. It is distinct from the ordinary legitimate interests basis and will only be used where the statutory conditions apply. As a public authority, the school will not

rely on legitimate interests or recognised legitimate interests where it is carrying out its public tasks if the law does not permit that basis.

For special category data, the school will also identify an appropriate condition under Article 9 UK GDPR and, where necessary, a corresponding condition under the Data Protection Act 2018. Criminal offence data will only be processed where the relevant requirements of Article 10 UK GDPR and the DPA 2018 are met.

Where the school relies on consent, consent will be specific, informed, freely given, unambiguous and capable of being withdrawn. The school will not use consent where another lawful basis is more appropriate.

7.2 Purpose limitation, minimisation and accuracy

- Only collect personal data that is necessary for a specified purpose.
- Explain the purpose and relevant information to individuals through appropriate privacy notices.
- Do not reuse personal data for an incompatible purpose without establishing that the further processing is lawful.
- Keep records accurate and provide appropriate routes for individuals to request correction.
- Delete, anonymise or securely dispose of information when it is no longer required, in line with the school's retention arrangements.

8. Privacy notices and transparency

The school will make appropriate privacy notices freely available to individuals whose personal data it processes. Privacy notices will explain, in clear language, what information is collected, why it is used, the lawful basis relied upon, retention arrangements, sharing, relevant rights and how to contact the school/DPO.

Privacy notices will be reviewed at least annually and whenever there is a significant change to how personal data is processed.

9. Sharing personal data

The school may share personal data where there is a lawful basis and appropriate safeguards. Sharing will be necessary, proportionate and limited to the information required for the purpose.

- Safeguarding and child protection purposes, where information needs to be shared to protect a child or another person.
- Legal obligations or official functions.
- Working with other agencies where there is a lawful basis and sharing is necessary.
- Providing school services through suppliers and processors.
- Emergency situations.
- Crime prevention or detection and other purposes permitted by law.

Where a processor is appointed, the school will carry out appropriate due diligence and ensure the required contractual data protection terms are in place. Where appropriate, the school will use a data sharing agreement or other documented arrangement.

Personal data will only be transferred outside the UK where the requirements of UK data protection law are met and appropriate safeguards are in place.

10. Information rights

Individuals have a range of rights under data protection law, depending on the circumstances. These may include the right to be informed, access personal data, request rectification, request erasure, restrict processing, object to processing, data portability and rights relating to automated decision-making.

Not every right is absolute and the availability of a right depends on the lawful basis and circumstances of the processing. Requests will be assessed under the current legislation and ICO guidance.

10.1 Subject access requests

A subject access request (SAR) may be made verbally or in writing. It does not need to use the words “subject access request” or refer to the UK GDPR. Staff who receive a request that may be an information rights request must forward it to the DPO or nominated person without delay.

The school will make reasonable and proportionate searches for the requested information. It will respond without undue delay and normally within one month. Where reasonably necessary to identify the information or processing activities concerned, the school may request clarification; the statutory time limit can be paused while clarification is awaited. Where a request is complex or numerous, the response period may be extended by up to a further two months, with the requester informed within the initial month.

The school will normally provide information free of charge. A reasonable fee may be charged, or a request may be refused, only where permitted by law, such as where a request is manifestly unfounded or excessive.

The school may need to verify identity, but will only request information that is reasonable and proportionate.

10.2 Children and subject access requests

Personal data belongs to the child to whom it relates. A child may exercise their right of access if they are considered competent to understand the nature and implications of the request. Where a parent or carer makes a request on behalf of a child, the school will consider the child's age, maturity and understanding, the nature of the information and any relevant legal authority. There is no fixed age at which a child is automatically considered competent.

Where a request concerns information about other people, the school will consider third-party rights and any applicable exemptions before disclosure.

11. Parental access to education records

Belmont is a maintained school in England and is therefore subject to the Education (Pupil Information) (England) Regulations 2005 concerning access to education records.

A person with parental authority may request access to a pupil's education record under those regulations. This is a separate right from the UK GDPR right of access. Written requests should be made to the school/DPO. The school will deal with requests within the statutory timescale, currently 15 school days, and will apply any exemptions and charging provisions permitted by the regulations.

ICO guidance: Accessing pupils' information

12. Photographs, videos and CCTV

The school may take photographs and videos of pupils and staff for educational, safeguarding, operational, communications or promotional purposes. The lawful basis will be determined for the particular purpose. Consent may be used where appropriate, particularly for optional publicity or promotional uses, but consent is not automatically required for every image or video taken in school.

Where consent is relied upon, it will be clear what the consent covers and individuals will be able to withdraw it where applicable. Withdrawal of consent will not affect processing that has already taken place lawfully.

The school will take reasonable steps to avoid publishing unnecessary identifying information alongside images. Images and videos will be stored and shared securely and retained only for as long as necessary.

Where CCTV is used, the school will have appropriate signage, lawful basis, retention arrangements, access controls and procedures for responding to requests. CCTV will only be used for specified purposes and in accordance with current data protection guidance.

13. Data protection by design, DPIAs and new technology

The school will consider data protection and privacy at the start of new projects and when changing existing systems or processing activities.

- A data protection impact assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms.
- The DPO will advise on whether a DPIA is required and on appropriate safeguards.
- The school will maintain an up-to-date record of processing activities and information asset/register arrangements.
- Before procuring new educational technology or other systems that process personal data, the school will consider data protection, security, contractual arrangements, data location, retention and deletion.
- The school will consider the additional privacy risks associated with generative AI and will follow its approved AI and acceptable-use arrangements.

14. Data security and storage

The school will protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. Security measures will be proportionate to the risks presented by the processing.

- Confidential papers will not be left where unauthorised people can access them.

- Access to electronic systems will be controlled through appropriate authentication and access permissions.
- Portable devices and removable media will be protected using appropriate encryption and security controls where required.
- Staff, governors and pupils must not store school personal data on personal devices or accounts unless this is specifically authorised and appropriate safeguards are in place.
- Personal data will only be shared through approved and secure methods.
- Access will be limited to people who need the information for legitimate school purposes.

Technical security requirements will be maintained through the school's ICT/cyber-security arrangements and will be reviewed as technology and official guidance develop.

15. Retention and disposal

Personal data will be retained only for as long as necessary and in accordance with the school's records management and retention schedule. Retention periods will take account of statutory requirements, safeguarding needs, legal claims, operational requirements and the public interest.

The school will review the personal data it holds and securely delete, destroy or anonymise information when it is no longer required. Where a record must be retained for a defined period, the reason for retention and applicable period should be documented.

16. Personal data breaches

All suspected or actual personal data breaches must be reported to the DPO or nominated data protection lead immediately. Examples include information being sent to the wrong person, loss or theft of a device containing personal data, unauthorised access, accidental publication, or inappropriate disclosure of safeguarding information.

The DPO will assess the breach, contain and mitigate its effects, document the incident and decide whether notification to the ICO is required. Where a breach is likely to result in a risk to individuals' rights and freedoms, the ICO will normally be notified without undue delay and, where required by law, within 72 hours of the school becoming aware of the breach.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay where required by law. All breaches will be documented, including those that are not reported to the ICO.

The detailed breach response procedure is set out in Appendix 1.

17. Training and awareness

All staff and governors will receive appropriate data protection information as part of induction and ongoing training. Additional training will be provided where legislation, guidance, technology, school processes or identified risks make this necessary.

The school will maintain appropriate records of data protection training and will promote a culture in which staff feel able to report concerns and seek advice.

18. Monitoring, accountability and review

The DPO and school leadership will monitor compliance with this policy and related procedures. The school will use appropriate records, audits, training records, breach logs, DPIAs, privacy notices and records of processing to demonstrate accountability.

This policy will be reviewed at least annually and sooner where legislation, official guidance, technology or school practice changes. It will be presented to the governing body for approval/review in accordance with the school's governance arrangements.

19. Complaints

Individuals who have concerns about how Belmont processes their personal data should contact the school/DPO in the first instance. Complaints will be handled promptly, fairly and in accordance with the school's data protection complaints procedure and current legal requirements.

Individuals also have the right to complain to the Information Commissioner's Office if they remain dissatisfied with the school's handling of their personal data.

ICO: Information Commissioner's Office

20. Contacts

For questions about this policy or data protection at Belmont Community Primary School, contact:

- Mrs Jenny Smeaton – School Business Manager
- Darrel Towndrow – Data Protection Officer

Appendix 1 – Personal Data Breach Procedure

This procedure should be followed whenever a suspected or actual personal data breach is identified.

- Report the suspected breach immediately to the DPO or nominated data protection lead. Staff should not delay reporting while attempting to investigate the incident themselves.
- Record the basic facts: what happened, when it happened, what information was involved, who may be affected and what immediate action has been taken.
- The DPO will assess whether a personal data breach has occurred and will identify the nature and scope of the incident.
- Contain the breach and take reasonable steps to recover, secure or restrict access to the information.
- Assess the likelihood and severity of the risk to individuals' rights and freedoms, taking account of the type and sensitivity of the information and the people affected.
- Decide whether the ICO must be notified. Where notification is required, it will normally be made without undue delay and, where applicable, within 72 hours of the school becoming aware of the breach.
- If the breach is likely to result in a high risk to individuals' rights and freedoms, determine whether affected individuals need to be informed without undue delay.

- Document the breach and the school's decision-making, including where the decision is not to notify the ICO.
- Identify and implement measures to prevent recurrence, such as changes to processes, access controls, training or technical safeguards.
- Review the incident with the relevant senior leader and DPO and ensure any lessons are incorporated into school procedures.

Appendix 2 – Key associated documents

- Staff and pupil privacy notices.
- Data retention schedule / records management arrangements.
- Record of processing activities and information asset register.
- Data breach log and breach reporting procedure.
- Data Protection Impact Assessment procedure/template.
- ICT/cyber-security and acceptable-use arrangements.
- Filtering and monitoring arrangements.
- AI / generative AI acceptable-use arrangements.
- Data sharing agreements and processor contracts, where applicable.
- Subject access request and other information-rights procedures.

Policy approval and review record

Date	Action	Approved / noted by
May 2025	Previous policy ratified	Full Governing Body
1 October 2026	2026/27 policy approved	Full Governing Body
1 October 2027	Next review	Full Governing Body