ST. GERARD'S CATHOLIC PRIMARY SCHOOL

DATA PROTECTION POLICY

Our Mission Statement

'With Christ at our side and St Gerard as our guide, we live, love, learn and pray together."

Approved by:	Governing Body	Date: September 2026
Next review due by:	September 2028	

Contents

1. Aims and scope
2. Legislation and guidance
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Data protection principles
7. Lawful processing and collecting personal data
8. Sharing personal data
9. Individual rights and subject access requests
10. Parental requests to see the educational record
11. Photographs and videos
12. Data protection by design and default
13. Data security and storage
14. Retention and disposal
15. Personal data breaches
16. Data protection complaints
17. Training
18. Monitoring and review
19. Links with other policies
Appendix 1: Personal data breach procedure

1. Aims and scope

St. Gerard's Catholic Primary School is committed to protecting the personal data of pupils, parents and carers, staff, governors, volunteers, visitors and other individuals. The school will collect, store, use and dispose of personal data lawfully, fairly, transparently and securely.
This policy applies to all personal data processed by the school, whether held electronically or in paper records, and to all staff, governors, volunteers, contractors and other individuals processing personal data on the school's behalf.
The policy should be read alongside the school's privacy notices, retention schedule, information security arrangements, safeguarding and online safety policies, and any procedures for handling information rights requests and data breaches.

2. Legislation and guidance

The school complies with UK data protection law, including:

- UK General Data Protection Regulation (UK GDPR), as amended from time to time.
- Data Protection Act 2018 (DPA 2018).
- Data (Use and Access) Act 2025 (DUAA), which amends the UK GDPR and DPA 2018.
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable.
- Education (Pupil Information) (England) Regulations 2005, including provisions relating to access to educational records.

The school follows relevant guidance from the Information Commissioner's Office (ICO) / Information Commission, the Department for Education (DfE), and other appropriate education-sector guidance. The DUAA does not replace the UK GDPR or DPA 2018; it amends aspects of the existing data protection framework. All data protection provisions relevant to organisations are now in force.
The school will keep this policy and associated procedures under review as further statutory guidance and regulatory guidance is issued.

3. 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 data, and data concerning sex life or sexual orientation.
Processing	Anything done with personal data, including collecting, recording, organising, storing, adapting, retrieving, using, sharing, restricting, erasing or destroying it.
Data subject	The identified or identifiable individual to whom personal data relates.
Data controller	The person or 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration,

	unauthorised disclosure of, or access to personal data.
DPIA	A Data Protection Impact Assessment, used to identify and minimise data protection risks arising from processing activities, particularly where processing is likely to result in a high risk to individuals.

4. The data controller

St. Gerard's Catholic Primary School is the data controller for personal data processed by the school in connection with its functions.
The school will maintain its registration and data protection fee arrangements with the ICO as required by law.
The school's Data Protection Officer (DPO) is Jonjo Wilson, contactable via jwilson@stgerard.bham.sch.uk.

5. Roles and responsibilities

5.1 Governing body

- Has overall responsibility for ensuring that the school complies with applicable data protection obligations.
- Receives appropriate assurance and reports from the DPO.

5.2 Data Protection Officer

- Oversees implementation of this policy and monitors compliance.
- Provides advice on data protection law, DPIAs, privacy information, information rights and data sharing.
- Acts as a key point of contact for individuals and the ICO/Information Commission.
- Maintains appropriate records of data breaches and data protection complaints.
- Advises on training, audits, retention and data protection by design.

5.3 Headteacher

- Provides day-to-day leadership and ensures appropriate resources and systems are in place.

5.4 All staff and governors

- Must process personal data only as necessary for their role and in accordance with this policy.
- Must keep personal data secure and report actual or suspected breaches immediately to the DPO.
- Must not disclose personal data to third parties unless authorised and lawful.
- Must refer information rights requests and data protection complaints to the DPO promptly.
- Must complete required data protection training.
- Must seek advice from the DPO before introducing new processing, technologies or data-sharing arrangements that may affect privacy.

6. Data protection principles

Personal data must be:

- 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;
- kept for no longer than is necessary; and

- processed securely, using appropriate technical and organisational measures.

The school will also comply with the accountability requirements of data protection law and be able to demonstrate how it complies.

7. Lawful processing and collecting personal data

The school will identify and document an appropriate lawful basis before processing personal data. Depending on the circumstances, these may include:

- consent
- contract
- legal obligation
- vital interests
- public task
- legitimate interests, where applicable
- recognised legitimate interests introduced by the DUAA, where the statutory conditions are met

The school will not rely on consent where another lawful basis is more appropriate. Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and individuals must be able to withdraw it. Special category data requires both an Article 6 lawful basis and an applicable Article 9 condition. Criminal offence data will be processed only where an appropriate lawful basis and condition under the DPA 2018 are satisfied.
When collecting personal data directly from individuals, the school will provide appropriate privacy information. Privacy notices will explain, as appropriate, what information is collected, why it is used, the lawful basis, who it is shared with, retention, individual rights and how to complain.

8. Sharing personal data

The school may share personal data where there is a lawful basis and where sharing is necessary and proportionate. Consent is not always required; for example, information may need to be shared to meet a legal obligation, perform a public task, protect vital interests, safeguard children or adults, or comply with a lawful request.
When using processors, the school will carry out appropriate due diligence and have a written contract containing the required data protection provisions. Only information necessary for the service will be shared.
The school may share information with the police, local authority, health services, social care, safeguarding partners, government bodies and other agencies where lawful and appropriate.
International transfers will be managed in accordance with the UK GDPR, DPA 2018 and current requirements concerning UK data protection safeguards.

9. Individual rights and subject access requests

Individuals have rights under data protection law, subject to applicable exemptions. These may include rights to access personal data, rectification, erasure, restriction, objection, data portability and rights relating to automated decision-making, where applicable.
All subject access requests (SARs), whether written, electronic or verbal, must be passed to the DPO without delay.
The school will carry out reasonable and proportionate searches when responding to SARs. Where clarification is reasonably required to identify the information requested, the statutory time period may be paused in accordance with current law.
The school will normally respond without undue delay and within the applicable statutory period. The DPO will determine whether an extension is permitted for a complex or numerous request and will explain this to the requester where required.
The school will not normally charge a fee for a SAR. A reasonable fee may be charged, or a request refused, where the request is manifestly unfounded or excessive, in accordance with data protection law.
The school may withhold information where an exemption applies, including where disclosure would reveal another person's personal data or where specific safeguarding, legal or other exemptions apply.

A child's right to access their personal data depends on their maturity and understanding. Requests made by parents or carers will be considered case by case, taking account of the child's rights and interests.
Staff must not attempt to respond to a SAR themselves unless directed by the DPO.

10. Parental requests to see the educational record

Parents and those with parental responsibility may have statutory rights to access their child's educational record under the Education (Pupil Information) (England) Regulations 2005. Requests will be handled in accordance with the Regulations and any applicable exemptions.
The school will distinguish between a request for an educational record and a subject access request and will seek advice from the DPO where the position is unclear.

11. Photographs and videos

The school may take photographs and record video as part of its educational, safeguarding, communication and promotional activities. The school will identify an appropriate lawful basis and provide appropriate privacy information for each use.
Where consent is the lawful basis, the school will obtain and manage consent appropriately and respect withdrawals of consent. Staff must follow the school's arrangements for photography, video, social media and communications.
Parents and carers taking photographs at school events for personal use should respect the privacy and safeguarding of other children and must not publish images of other pupils without appropriate permission.

12. Data protection by design and default

The school will consider privacy and data protection at the start of new projects, systems and activities rather than as an afterthought.

- A DPIA will be completed where required and where processing is likely to result in a high risk to individuals.
- Only the minimum personal data necessary for the purpose will be collected and used.
- Access to personal data will be restricted according to role and need.
- Privacy information will be updated when processing changes.
- The school will consider the specific higher-protection requirements concerning children where relevant.
- New technologies, including AI-enabled tools, will be risk assessed and approved through the school's data protection processes before personal data is entered or shared.

13. Data security and storage

The school will use appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- Paper records containing confidential information must be stored securely and not left accessible to unauthorised people.
- Portable devices and removable media containing personal data must be appropriately secured and encrypted where required.
- Staff must use strong, unique passwords and follow the school's information security arrangements.
- Personal data must not normally be stored on personal devices or personal cloud services.
- Information taken off site must be kept secure and returned or deleted when no longer required.
- Personal data must only be shared through approved systems and with appropriate safeguards.
- Access rights will be reviewed and removed when no longer required.

14. Retention and disposal

The school will retain personal data only for as long as necessary and in accordance with its records retention schedule and applicable statutory requirements.
When records are no longer required, they will be securely destroyed, deleted or anonymised. Disposal arrangements will also apply to records held by processors acting on the school's behalf.

15. Personal data breaches

A personal data breach or suspected breach must be reported immediately to the DPO. Examples include information being sent to the wrong person, loss or theft of a device, unauthorised access, accidental disclosure, or personal data being published without authorisation.
The DPO will assess the breach, contain it, document the decision-making and determine whether notification to the ICO/Information Commission is required. Where notification is required, it will normally be made without undue delay and, where feasible, within 72 hours of the school becoming aware of the breach.
The school will notify affected individuals where required by law and will keep a record of all personal data breaches, whether or not they are reportable.

16. Data protection complaints

The school recognises the statutory right of individuals to complain directly to the school about the handling of their personal data.
Data protection complaints should be directed to the DPO at jwilson@stgerard.bham.sch.uk. The school will provide an accessible means of submitting a complaint, acknowledge the complaint within the required period, investigate it appropriately and respond without undue delay.
The school will keep appropriate records of data protection complaints and the action taken. Individuals also retain the right to complain to the ICO/Information Commission if they remain dissatisfied.
Data protection complaints are distinct from ordinary school complaints, although the school may use its established complaints framework where appropriate, provided that the specific statutory data protection requirements are met.

17. Training

All staff and governors will receive appropriate data protection training as part of induction and periodically thereafter. Additional training will be provided where legislation, guidance, systems or school procedures change. The Policy and updates will be shared annually.

18. Monitoring and review

The DPO is responsible for monitoring and reviewing this policy, taking account of changes in legislation, ICO/Information Commission guidance, DfE guidance, school systems and identified risks.
The policy will be reviewed at least annually, or sooner where a significant legal, regulatory or operational change occurs, and will be presented to the governing body for approval.

19. Links with other policies

- Freedom of Information Publication Scheme
- Online Safety Policy
- Child Protection and Safeguarding Policy
- Records Retention Schedule
- Privacy Notices
- Acceptable Use / ICT arrangements
- Complaints Policy
- Artificial Intelligence Policy, where applicable

Appendix 1: Personal data breach procedure

1. Any staff member, governor, volunteer or processor who identifies or causes an actual or suspected personal data breach must immediately notify the DPO.
2. The DPO will establish the facts, identify the information involved and take immediate steps to contain the breach.
3. The DPO will assess the likelihood and severity of the risk to individuals and document the assessment.
4. The DPO will determine whether notification to the ICO/Information Commission is required and, where required, make the notification within the applicable statutory timeframe.
5. Where a breach is likely to result in a high risk to individuals, the DPO will determine whether affected individuals must be informed and will ensure appropriate communication.
6. All breaches will be documented, including those that are not reported to the regulator.
7. The DPO and relevant senior leaders will review the incident and identify actions to reduce the likelihood of recurrence, including changes to systems, procedures or training.
8. Where a processor is involved, the school will ensure that the processor fulfils its contractual and legal obligations and provides the information needed for the school to meet its duties.

Policy note: This policy is intended to reflect the school's current data protection arrangements and UK data protection framework as at September 2026. It should be read alongside the school's current privacy notices, retention schedule, breach procedure and advice from the school's appointed data protection adviser/DPO.