Bradford Christian School

Data Protection and Cyber Security Policy

Policy rewritten: October 2025 **Review Date:** October 2026

Contents

Appendices:

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors, and other individuals is collected, stored, and processed in accordance with UK data protection law.

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

The school recognises that effective data protection and cyber security are essential to:

- Protect the privacy and rights of individuals
- Maintain trust within our school community
- Comply with legal obligations
- Safeguard our systems, staff, and learners from cyber threats

2. Legislation and Guidance

This policy meets the requirements of:

- **UK General Data Protection Regulation (UK GDPR)** – The EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- **Data Protection Act 2018 (DPA 2018)**

It is based on guidance published by:

- The Information Commissioner's Office (ICO) on the UK GDPR
- The Department for Education (DfE) on generative artificial intelligence in education
- The ICO's guidance for the use of surveillance cameras and personal information

This policy also has regard to:

- **Keeping Children Safe in Education (KCSIE) 2025**, particularly:
    - Paragraphs 107-120 on information sharing for safeguarding
    - Paragraphs 139-148 on online safety, filtering and monitoring
    - Paragraph 144 on cyber security
- **Working Together to Safeguard Children 2023** on information sharing
- **The Cyber Security Standards for Schools and Colleges**, developed to help schools improve their resilience against cyber-attacks
- **Guidance from the National Cyber Security Centre (NCSC)**
- **Guidance from the National Education Network** on e-security
- **The Department for Education's Filtering and Monitoring Standards**
- **ICO guidance** on data security and cyber incidents

Note: As an independent school, the school must comply with the UK GDPR and DPA 2018. While this policy references the Education (Pupil Information) (England) Regulations 2005, the school's specific approach to educational records is detailed in Section 10.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's name, ID number, location data, online identifier (username), or factors specific to their physical, mental, economic, cultural, or social identity.
Special categories of personal data	Personal data which is more sensitive and requires more protection, including information about an individual's: Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Health (physical or mental), Sex life or sexual orientation, Genetic data, Biometric data (where used for identification purposes).
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data (i.e., the school).
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller (e.g., an outsourced IT provider, cloud storage provider, exam board).
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Impact Assessment (DPIA)	A process to help identify and minimise data protection risks of a project or plan, particularly where new technologies are being introduced or where processing is likely to result in high risk to individuals' rights and freedoms.

4. The Data Controller

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors, and others, and therefore is a data controller.

The school is registered with the ICO and has paid its data protection fee, as legally required.

5. Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Board

The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection and cyber security obligations and approves this policy.

The Governing Board will:

- Ensure adequate resources are allocated to data protection and cyber security
- Receive regular reports from the DPO on compliance and incidents
- Review and approve this policy annually
- Ensure appropriate training is provided to governors on their data protection responsibilities
- Provide strategic oversight of the school's data protection and cyber security arrangements

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Board and act as the first point of contact for individuals and the ICO.

Our DPO is: Shaun McGrail
Contact: dpo@bxs.org.uk

The DPO's responsibilities include:

- Monitoring compliance with UK data protection law
- Advising on Data Protection Impact Assessments (DPIAs) (but not carrying them out)
- Advising on the school's obligations regarding data breach reporting
- Acting as the contact point for the ICO
- Taking a risk-based approach to data protection
- Conducting regular cyber security audits
- Maintaining logs of data breaches and security incidents
- Providing guidance and support to staff on data protection matters
- Reviewing and updating privacy notices
- Maintaining the register of data processors
- Coordinating responses to subject access requests
- Delivering or arranging data protection training

The school ensures that the DPO:

- Operates independently and is not dismissed or penalised for performing their duties
- Is closely involved, in a timely manner, in all issues relating to the protection of personal data
- Is provided with necessary resources to fulfil their obligations and maintain their expert knowledge
- Reports directly to the highest level of management (the Governing Board)
- Has no conflict of interest in their role

5.3 Headteacher

The Headteacher acts as the representative of the Data Controller on a day-to-day basis and works with the DPO to ensure the school's data protection and cyber security measures are effective.

5.4 All Staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Immediately contacting the DPO if a data breach occurs or is suspected
- Contacting the DPO with any questions or concerns regarding the use, retention, security, or transfer of personal data
- Following all cyber security procedures outlined in this policy

- Reporting any suspicious emails, messages or cyber security concerns immediately
- Completing all required data protection and cyber security training
- Not assuming that someone else will take action on data protection or safeguarding concerns

6. Data Protection Principles

The UK GDPR is based on seven data protection principles that our school must comply with. The Data Protection Act 2018 and UK GDPR place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure.

Personal data must be:

1. **Processed lawfully, fairly and in a transparent manner** (Lawfulness, Fairness and Transparency)
2. **Collected for specified, explicit and legitimate purposes** (Purpose Limitation)
3. **Adequate, relevant and limited to what is necessary** (Data Minimisation)
4. **Accurate and, where necessary, kept up to date** (Accuracy)
5. **Kept for no longer than is necessary** (Storage Limitation)
6. **Processed in a way that ensures it is appropriately secure** (Integrity and Confidentiality)

In addition, the school must comply with the principle of **Accountability** by demonstrating that we meet all the above principles through:

- Maintaining appropriate documentation
- Implementing appropriate policies and procedures
- Conducting regular audits and reviews
- Providing staff training
- Implementing data protection by design and default

7. Collecting Personal Data

7.1 Lawfulness, Fairness, and Transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under Article 6 of the UK GDPR:

1. **Contract:** The data needs to be processed so that the school can fulfil a contract with the individual (or take pre-contractual steps)
2. **Legal Obligation:** The data needs to be processed so that the school can comply with a legal obligation
3. **Vital Interests:** The data needs to be processed to protect someone's life

4. **Public Task:** The data needs to be processed so that the school can perform a task in the public interest or exercise its official authority (this is the most common basis for schools)
5. **Legitimate Interests:** The data needs to be processed for the legitimate interests of the school or a third party, provided the individual's rights and freedoms are not overridden
6. **Consent:** The individual (or their parent/carer, where appropriate) has freely given clear consent

For special categories of personal data (e.g., health, ethnic origin, religious beliefs, biometric data), we must also meet one of the special category conditions for processing under Article 9 of the UK GDPR, such as:

- Explicit consent
- Substantial public interest
- For health or social care purposes
- To protect vital interests where the data subject is incapable of giving consent
- For reasons of public interest in the area of public health

When we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law via a privacy notice.

7.2 Limitation, Minimisation, and Accuracy

We will only collect personal data for specified, explicit, and legitimate reasons.

Staff must only process personal data where it is necessary in order to do their jobs. Staff should not collect or retain personal data "just in case" it might be useful.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate. Staff should inform the school office immediately if they become aware of inaccurate personal data.

Personal data no longer needed will be deleted or anonymised in accordance with the school's record retention schedule (see Appendix 2).

7.3 Automated Decision-Making and Profiling

Our school does not use automated decision-making or profiling in relation to any personal data we process. All decisions that may have legal or similarly significant effects on individuals involve human intervention and oversight.

If we introduce any automated decision-making or profiling in the future, we will:

- Update this policy
- Inform affected individuals through updated privacy notices
- Ensure appropriate safeguards are in place

- Conduct a DPIA
- Provide information about the logic involved and the significance and envisaged consequences
- Provide individuals with the right to human intervention

7.4 Privacy Notices

We provide clear and transparent information to individuals about how we use their personal data through separate privacy notices for:

- Pupils and parents/carers
- Staff (including volunteers and governors)
- Visitors and contractors
- Job applicants

Our privacy notices:

- Are published on the school website
- Are provided to individuals when we first collect their personal data
- Explain the lawful basis for processing
- Explain how long data will be retained
- Explain individuals' rights
- Explain how to contact the DPO
- Are reviewed and updated at least annually or when there are significant changes to our processing activities

8. Sharing and Transferring Personal Data

The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. If in any doubt about sharing information, staff should speak to the designated safeguarding lead (or a deputy). Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children. We will not normally share personal data with anyone else without consent, but we may be required to do so where:

- There is an immediate risk of harm or a safety risk to staff or pupils
- We need to liaise with other agencies (e.g., safeguarding referrals to children's social care)
- We are legally required to share data with law enforcement or government bodies
- It is necessary for the performance of a task carried out in the public interest
- It is necessary for the purposes of our legitimate interests (where applicable and appropriate)

8.1 Information Sharing for Safeguarding

As a school, we have clear powers to share, hold and use information for the purposes of identifying and tackling all forms of abuse, neglect, and exploitation, and in promoting children's welfare, including in relation to their educational outcomes.

School staff should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children's social care.

We can share information with the appropriate people if we believe that doing so is likely to support the safeguarding and protection of a child. We will only share information that is relevant and necessary, and only with individuals, agencies or organisations that have a role in safeguarding the child and/or providing support to their family.

We must not share information if it may harm a child or put them at risk of harm.

When sharing safeguarding information, we will:

- Only share relevant information needed to support the provision of services
- Be transparent with the child and/or their family where it is safe and appropriate to do so
- Share information quickly in urgent cases where there is an immediate risk to the child
- Record the reasons for our information sharing decision, whether we share or not
- Seek advice from our Designated Safeguarding Lead or DPO if we are uncertain
- Not assume that someone else will share the information

Staff responsibilities:

Staff should not assume a colleague, or another professional will take action and share information that might be critical in keeping children safe. They should be mindful that early information sharing is vital for the effective identification, assessment, and allocation of appropriate service provision, whether this is when problems first emerge, or where a child is already known to local authority children's social care.

This approach is in accordance with Keeping Children Safe in Education 2025 (paragraphs 107-120) and Working Together to Safeguard Children 2023.

8.2 Data Processing Agreements (Contracts)

Whenever our school (the data controller) shares data with a third party (a data processor), such as an exam board, IT service provider, cloud storage provider, or payroll provider, we will ensure that a written contract (Data Processing Agreement) is in place before any personal data is shared.

These contracts ensure the processor:

- Acts only on our written instruction
- Maintains confidentiality

- Takes appropriate technical and organisational security measures
- Ensures the deletion or return of data when the contract ends
- Notifies us immediately of any personal data breach
- Assists us in responding to requests from data subjects exercising their rights
- Makes available all information necessary to demonstrate compliance with data protection obligations
- Does not engage sub-processors without our written authorisation
- Allows us to conduct audits and inspections where appropriate
- Complies with UK GDPR and DPA 2018

8.3 International Data Transfers

Our school assigns staff and students a Google Workspace account. We acknowledge that data is stored across a global network of data centres owned by Google, which constitutes a transfer outside the UK.

We rely on appropriate safeguards provided by Google, including Standard Contractual Clauses (SCCs) approved by the ICO, to ensure this transfer is compliant with UK data protection law.

If other international transfers become necessary, we will ensure appropriate safeguards are in place in accordance with UK data protection law, such as:

- Adequacy decisions (where the ICO has determined that a country provides adequate protection)
- Standard Contractual Clauses
- Binding Corporate Rules (where applicable)

We will not transfer personal data outside the UK without appropriate safeguards in place.

8.4 Security of International Transfers

When data is transferred internationally (such as through our Google Workspace accounts), we ensure:

Encryption during transit: All data transfers use secure, encrypted connections (TLS/SSL protocols)

Verification of recipient security measures: We verify that recipients have appropriate technical and organisational security measures in place through:

- Review of their security certifications
- Assessment of their data protection policies
- Regular audits where contractually agreed

Legal basis for transfer: We rely on appropriate safeguards such as Standard Contractual Clauses or adequacy decisions

Documentation: We maintain records of all international transfers including:

- The categories of personal data transferred
- The countries to which data is transferred
- The safeguards in place
- Copies of relevant transfer mechanisms

Regular review: We regularly review third-party security certifications and compliance, at least annually

8.5 Third-Party Data Processors and Supplier Management

When engaging suppliers who will process personal data on our behalf, we will:

Due Diligence (Before Appointment):

- Conduct due diligence on their security measures and data protection practices
- Require evidence of cyber security certifications (e.g., Cyber Essentials, Cyber Essentials Plus, ISO 27001)
- Review their data protection and security policies
- Assess their track record of data breaches and security incidents
- Verify their compliance with UK GDPR and DPA 2018
- Check their insurance coverage for data breaches

Contractual Requirements:

Ensure Data Processing Agreements are in place before any data is shared, which must include:

- Requirement that the processor acts only on our written instructions
- Obligation to maintain confidentiality
- Specific security requirements including:
    - Encryption of data in transit and at rest
    - Access controls and authentication requirements (including multi-factor authentication where appropriate)
    - Incident notification procedures (immediate notification of any breach)
    - Right to audit security measures
    - Data deletion or return procedures when contract ends
    - Restrictions on sub-processing (requiring our written consent)
    - Staff training requirements for processor's staff
    - Compliance with our security standards
- Provisions for termination if security standards are not maintained
- Liability and indemnity clauses

Ongoing Monitoring:

- Conduct annual reviews of supplier security measures
- Monitor supplier compliance with contractual security requirements
- Review and update Data Processing Agreements when suppliers change their practices

- Maintain a register of all data processors including:
    - Name and contact details
    - Categories of data processed
    - Purpose of processing
    - Security measures in place
    - Date of last review
    - Any security incidents
- Request regular security audit reports from processors
- Conduct our own audits where contractually permitted

Supplier Changes:

Require suppliers to notify us immediately of any changes to:

- Their security measures or policies
- Sub-processors they use (we must provide written consent before any sub-processor is engaged)
- Location of data storage or processing
- Ownership or management structure
- Security certifications or accreditations

We will reassess security and data protection compliance when significant changes occur and may terminate the contract if changes pose unacceptable risks to personal data.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests (SARs)

Individuals have a right to make a Subject Access Request (SAR) to gain access to their personal information held by the school under Article 15 of the UK GDPR.

To make a SAR, please email or write to the School Office.

The School Business Manager will:

- Verify the identity of the person making the request
- Respond without undue delay and within one month of receipt
- Extend the deadline by up to two months if the request is complex or numerous (notifying the individual within the initial month, along with the reasons for the delay)
- Provide information free of charge unless the request is manifestly unfounded, excessive, or repetitive (in which case we may charge a reasonable fee or refuse to respond)

We will provide:

- Confirmation that we are processing the individual's personal data
- A copy of the personal data

- Information about the purposes of processing
- Information about the categories of data concerned
- Information about recipients or categories of recipients
- Information about retention periods
- Information about the individual's rights
- Information about the source of the data (if not collected directly from the individual)
- Information about any automated decision-making (if applicable)

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, not the parent or carer.

Under 12s: Children below the age of 12 are generally not regarded as mature enough to understand their rights, so requests from parents are usually granted without the pupil's express permission.

Aged 12 and above: Children aged 12 and above are generally regarded as mature enough to understand their rights, and their consent may be required before granting a parent's request.

A pupil's capacity to understand their rights will always be judged on a case-by-case basis, taking into account:

- The child's level of maturity and understanding
- The nature of the personal data
- Any relevant circumstances

9.3 Responding to Subject Access Requests

When responding to requests, we may refuse to disclose information for specific legal reasons under Schedule 2 of the DPA 2018, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would include another person's personal data that we cannot reasonably anonymise without their consent
- Is subject to legal professional privilege
- Would prejudice the prevention or detection of crime
- Is being used in connection with legal proceedings
- Relates to child abuse data and disclosure would not be in the best interests of the child

When we refuse a request (in whole or in part) or charge a fee, we will:

- Tell the individual why within one month
- Inform them of their right to complain to the ICO
- Inform them of their right to seek judicial remedy through the courts

9.4 Other Data Protection Rights

Individuals also have the right to:

Right to rectification: Ask us to rectify inaccurate or incomplete personal data without undue delay

Right to erasure ('right to be forgotten'): Ask us to erase their personal data in certain circumstances, such as:

- The data is no longer necessary for the purpose it was collected
- They withdraw consent (where consent was the lawful basis)
- They object to processing and there are no overriding legitimate grounds
- The data has been unlawfully processed
- The data must be erased to comply with a legal obligation

Right to restrict processing: Ask us to restrict processing of their personal data in certain circumstances, such as while we verify the accuracy of the data or assess whether we have legitimate grounds to process it

Right to object: Object to processing justified on the basis of public interest or legitimate interests, including for direct marketing purposes (we will stop processing unless we can demonstrate compelling legitimate grounds)

Right to data portability: Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances where processing is based on consent or contract and carried out by automated means)

Right to withdraw consent: Withdraw their consent at any time (where consent was the lawful basis for processing). We will stop processing the data unless we have another lawful basis for continuing to process it.

Rights related to automated decision-making: Not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects (our school does not currently use such processing)

9.5 Privacy and Electronic Communications (PECR)

We comply with the Privacy and Electronic Communications Regulations (PECR) for electronic communications used for marketing or promotional purposes.

We will:

- Actively seek consent from all recipients on our mailing lists before sending marketing communications
- Ensure recipients have the opportunity to withdraw consent/unsubscribe at any time
- Make the unsubscribe process simple and straightforward
- Include clear unsubscribe information in every marketing communication
- Process unsubscribe requests promptly (within one month)

- Not send marketing communications to individuals who have opted out

9.6 Freedom of Information (FOI)

The school proactively publishes information on the school website via our Publication Scheme, in accordance with the Freedom of Information Act 2000.

The school will aim to respond to all valid FOI requests within 20 working days.

10. Parental Requests to See the Educational Record

As an independent school, parents (or those with parental responsibility) do not have an automatic statutory right of access to the educational record kept by our school for their child under the Education (Pupil Information) (England) Regulations 2005.

However:

For pupils whose place is funded by a local authority (e.g., specific SEN funding): We recognise that we are bound by the Education (Pupil Information) (England) Regulations 2005 for that pupil's educational record. In these cases, parents have the statutory right to request a copy of the educational record within 15 school days of the request, and we may charge a fee not exceeding the cost of supply.

For all other pupils: While the statutory right does not apply, parents may still access the information via a Subject Access Request (SAR) under the UK GDPR, which will be provided free of charge within one month.

To request information from your child's educational record, you should apply in writing to the school office, clearly stating:

- Your relationship to the child
- The information you are requesting
- The format in which you would like to receive the information

All requests, regardless of the child's funding status, will be handled efficiently and strictly in line with the principles of the UK GDPR and the child's data protection rights.

11. CCTV

Our school uses Closed Circuit Television (CCTV) within the premises to ensure a safe and secure environment. The system does not use any sound recording capability.

11.1 Lawful Basis and Data Protection Impact Assessment

We rely on the 'public task' lawful basis under Article 6(1)(e) of the UK GDPR for operating CCTV, as it is necessary for us to perform our functions as an educational institution and to ensure the safety of our school community.

A Data Protection Impact Assessment (DPIA) has been completed for our CCTV system in accordance with Article 35 of the UK GDPR, as large-scale systematic monitoring of a publicly accessible area requires a DPIA. This assessment:

- Identifies and assesses risks to individuals' rights and freedoms
- Evaluates the necessity and proportionality of the processing
- Identifies measures to mitigate identified risks
- Is reviewed whenever significant changes are made to the system or its purposes

11.2 Purposes of Use

The school uses CCTV for the following specified, explicit, and legitimate purposes:

- To provide a safe and secure environment for pupils, staff, and visitors
- To protect the school buildings and assets
- To assist in the prevention and detection of crime
- To support the investigation of incidents
- To monitor activity for the purpose of securing the safety and well-being of the school community
- To monitor student behaviour where appropriate for safeguarding purposes

11.3 Signage and Transparency

We ensure that all individuals are aware when they are in an area under CCTV surveillance by:

- Placing prominent signs at the entrance of CCTV-monitored zones
- Reinforcing these with further signs within the monitored area
- Ensuring signs are clearly visible and readable

Signs include:

- The organisation operating the system (Bradford Christian School)
- The purpose for using CCTV
- Contact details for enquiries (dpo@bxs.org.uk)

11.4 Retention and Storage

All retained CCTV data will be:

- Stored securely on a secure central server with appropriate access controls
- Kept for a maximum of 30 days, after which it is automatically overwritten or deleted
- Retained for longer only if required for a specific investigation or legal proceedings (with appropriate justification documented and reviewed regularly)
- Protected by appropriate technical and organisational security measures
- Access and viewing restricted to authorised operators only, who have been appropriately trained

11.5 Access Rights

Individuals have the right to request access to CCTV footage of themselves under Article 15 of the UK GDPR (subject access request).

Such requests should be directed to the DPO at dpo@bxs.org.uk and must include:

- Sufficient information to identify the individual
- Specific details about when and where the footage was recorded (date, time, location)
- Proof of identity

We will respond to such requests within one month, unless the request is complex, in which case we may extend this by a further two months.

We may refuse a request where:

- We cannot identify the individual in the footage
- The footage includes other individuals who cannot be reasonably anonymised
- Disclosure would prejudice the prevention or detection of crime
- Disclosure would prejudice legal proceedings

11.6 Covert Monitoring

We do not currently use covert CCTV monitoring. If we were to consider this in exceptional circumstances, we would:

- Seek specialist legal advice
- Carry out a DPIA
- Ensure the issue is serious enough to justify covert monitoring
- Obtain authorisation from a senior leader
- Stop covert monitoring once the investigation is finished
- Comply with all relevant legislation

11.7 Enquiries

Any enquiries about the CCTV system should be directed to the DPO at dpo@bxs.org.uk.

12. Biometric Recognition Systems

Our school does not currently use any biometric recognition systems (such as fingerprint scanners for cashless catering or library systems).

12.1 Future Use

If we decide to introduce biometric systems in the future, we will fully comply with sections 26-28 of the Protection of Freedoms Act 2012 by ensuring:

Notification: We will notify parents/carers and pupils in writing before any biometric system is introduced, providing clear information about:

- What biometric information will be processed
- How it will be used
- Where it will be stored
- How long it will be retained
- The right to refuse or withdraw consent

Consent: We will obtain explicit written consent from:

- At least one parent/carer (for pupils under 18), **AND**
- The pupil themselves (if they are competent to understand - generally aged 12 or over)

Both consents are required. If either the pupil or a parent/carer refuses or withdraws consent, we will not process the biometric data.

Opt-Out: We will provide a reasonable alternative means of accessing the relevant service for any pupil who:

- Objects to the processing of their biometric data
- Whose parent/carer objects
- Who has not provided the required consent

The alternative method will not disadvantage the pupil or make them identifiable as someone who has not consented.

Pupil Refusal: We will not process the biometric data of a pupil where:

- They, or a parent/carer, object to such processing
- The pupil (even if under 18 and a parent has consented) objects
- Consent has been refused or withdrawn

Data Protection: Any biometric data collected will be:

- Processed in accordance with this policy and the UK GDPR as special category data
- Protected by appropriate technical and organisational security measures
- Stored securely and separately from other personal data
- Encrypted both in transit and at rest
- Deleted when the pupil leaves the school or when consent is withdrawn
- Not shared with any third parties without explicit consent
- Subject to a DPIA before implementation

13. Photographs and Videos

We may take photographs and record images of individuals as part of school activities.

13.1 Lawful Basis

For photographs and videos used for internal educational purposes (such as displays in classrooms, recording pupil progress , documenting learning activities), we rely on the **'public task'** lawful basis under Article 6(1)(e) of the UK GDPR.

For photographs and videos used for communication, marketing and promotional materials (such as on our website, social media, prospectuses, or in local media), we rely on **consent** as our lawful basis for processing under Article 6(1)(a) of the UK GDPR.

13.2 Use and Consent

We will obtain written consent from parents/carers (or from pupils aged 18 or over) before photographs and videos are taken of their child for:

- Communication purposes (e.g., newsletters, displays in public areas of the school)
- Marketing and promotional materials (e.g., prospectus, website, social media)
- Media coverage (e.g., local newspapers, television)

Our consent forms will clearly specify:

- What the images will be used for
- Where they will be published or displayed
- How long they will be retained
- How to withdraw consent
- That consent is freely given and can be refused

Withdrawal: Consent can be refused or withdrawn at any time. If consent is withdrawn, we will:

- Stop using the photograph or video for the specified purposes
- Remove it from our website and social media accounts where reasonably practicable
- Delete it from our systems where it is no longer needed for other legitimate purposes
- Not distribute it further

When using photographs and videos for marketing or promotional purposes, we will not accompany them with any other personal information about the child (such as their full name or other identifying details) to ensure they cannot be easily identified, unless specific consent has been given for this additional information to be published.

13.3 Safeguarding Considerations

We will not use photographs or videos of pupils where:

- There are safeguarding concerns that make it inappropriate
- A court order is in place restricting publication of images
- The child is in care and consent has not been obtained from the appropriate authority
- The child or their family is in a refuge or witness protection programme
- There are other specific safeguarding reasons documented by the Designated Safeguarding Lead

13.4 Parental/Carer Use at Events

We recognise that parents/carers may wish to take photographs or videos at school events for personal, family use.

We will:

- Inform parents/carers of our expectations before events
- Ask that photos or videos taken by parents/carers at school events for personal use are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed
- Explain that images should be for personal use only and should not be shared in ways that could identify other children without consent
- Reserve the right to prohibit photography/videography at certain events where safeguarding concerns make this necessary

13.5 Media and External Organisations

If the media or external organisations wish to take photographs or videos at school events, we will:

- Seek specific consent from parents/carers in advance
- Ensure that any media representatives are accompanied by a member of staff at all times
- Brief media representatives on our safeguarding requirements
- Provide media representatives with a list of pupils who cannot be photographed
- Ensure appropriate agreements are in place regarding use and retention of images

13.6 Staff Photographs

We will obtain consent from staff members before using their photographs or videos for:

- Marketing and promotional purposes
- Publication on our website or social media
- Media coverage

Staff photographs used for internal purposes (such as ID badges, staff information boards, internal communications) are processed under the 'legitimate interests' or 'public task' lawful basis.

14. Artificial Intelligence (AI)

The school recognises that AI tools pose risks to sensitive and personal data, and that AI technology is rapidly evolving. We are committed to using AI safely, responsibly, and in compliance with data protection law.

14.1 Lawful Basis for AI Processing

When using AI tools that process personal data, we will identify an appropriate lawful basis under Article 6 of the UK GDPR, typically:

- **Public task** (for educational purposes and school administration)
- **Legitimate interests** (where applicable and appropriate, with a legitimate interests assessment completed)
- **Consent** (for certain specific uses)

14.2 Controls and Restrictions

For Students:

- All public chatbots and generative AI tools are blocked to students on school networks
- Google Gemini (if available through our Google Workspace for Education licence) may only be used under supervised conditions and for approved educational purposes
- Students receive age-appropriate training on the safe and responsible use of AI
- Use of AI tools by students is supervised and monitored
- Students are taught about the risks of entering personal information into AI tools

For Staff:

- Staff must only use AI tools that have been approved by the school and appear on our approved AI tools list
- **Personal and/or sensitive data must never be entered into any unauthorised generative AI tool**
- Staff receive regular training on the risks associated with AI and how to use approved tools safely
- Staff understand that AI tools can be used by cyber attackers to create more convincing scam emails

14.3 Risk Assessment for AI Tools

Before introducing any new AI tool that will process personal data, the school will carry out a Data Protection Impact Assessment (DPIA) if the processing is likely to result in a high risk to individuals' rights and freedoms, in accordance with Article 35 of the UK GDPR.

This assessment will include:

- Verification of the supplier's data protection and security credentials
- Review of how the AI tool processes, stores and shares data
- Assessment of whether the AI tool uses personal data for training purposes
- Evaluation of risks to individuals' rights and freedoms, including:
    - Data protection and privacy risks
    - Safeguarding and online safety risks
    - Cyber security risks
    - Academic integrity and misinformation risks
    - Equality and bias risks
    - Intellectual property risks
- Identification of measures to mitigate identified risks
- Ensuring appropriate Data Processing Agreements are in place
- Review of privacy settings and data sharing options
- Assessment of the necessity and proportionality of using the AI tool
- Consideration of the ethical implications of using AI in an educational setting

14.4 Approved AI Tools

The school maintains a list of approved AI tools that have undergone appropriate security and data protection assessments. This list:

- Is reviewed termly by the DPO and updated as necessary
- Is available from the DPO upon request
- Clearly specifies what each tool can and cannot be used for
- Is communicated to all staff through training and regular updates

Currently approved AI tools include:

- Google Gemini (via Google Workspace for Education) - for supervised educational use only

Staff must not use AI tools that are not on the approved list without prior written approval from the DPO.

14.5 Data Processing Agreements for AI Tools

For all AI tools that process personal data on our behalf, we will ensure that:

- Appropriate Data Processing Agreements are in place before any personal data is processed
- The supplier provides clear information about:
    - What data is processed
    - How data is stored and secured
    - Whether data is used for training AI models (and if so, how to opt out)
    - Data retention periods
    - Data deletion procedures
    - Geographic location of data processing and storage
- The supplier complies with UK GDPR and DPA 2018

- The supplier has appropriate security certifications

14.6 Transparency and Privacy Notices

We will update our privacy notices to inform individuals when AI tools are used to process their personal data, including:

- What AI tools are used
- For what purposes
- What categories of data are processed
- Whether any automated decision-making takes place
- How individuals can exercise their rights

14.7 Data Breach Protocol

If personal and/or sensitive data is entered into an unauthorised generative AI tool, our school will treat this as a data breach and will follow the procedure outlined in Appendix 1.

This includes:

- Immediate reporting to the DPO
- Assessment of the risk to individuals
- Containment measures where possible (e.g., requesting deletion from the AI provider)
- Notification to the ICO if required (within 72 hours)
- Notification to affected individuals if required
- Review of controls to prevent recurrence
- Additional training for staff involved

15. Data Protection by Design and Default

We integrate data protection into all processing activities from the design stage, in accordance with Article 25 of the UK GDPR, including:

- **Appointing a suitably qualified DPO** with the necessary resources, independence and authority to perform their role effectively
- **Only processing personal data that is necessary** (data minimisation) for the specific purpose - staff should not collect data "just in case"
- **Completing a Data Protection Impact Assessment (DPIA)** before any processing activity that is likely to result in a high risk to individuals' rights and freedoms, including:
    - Use of new technologies (including AI)
    - Large-scale processing of special category data
    - Systematic monitoring (such as CCTV)
- **Regularly training members of staff** on data protection and cyber security (see Section 19)

- **Maintaining records of processing activities** to demonstrate accountability
- **Implementing appropriate technical and organisational measures** to ensure data security by default
- **Reviewing and updating our data protection practices** regularly to ensure continued compliance
- **Considering data protection implications** when procuring new systems or services
- **Building privacy into our systems and processes** from the outset, rather than as an afterthought
- **Implementing privacy-enhancing technologies** where appropriate (e.g., pseudonymisation, encryption)
- **Conducting regular audits** of our data processing activities
- **Ensuring data protection is considered** in all policy development and decision-making
- **Minimising access to personal data** through role-based access controls
- **Ensuring default settings** are the most privacy-friendly options
- **Documenting our data protection decisions** to demonstrate accountability

16. Data Security and Remote Working

We will protect personal data and keep it safe from unauthorised access, accidental loss, destruction or damage, in accordance with Article 32 of the UK GDPR.

16.1 Physical Security

- Paper records containing personal data are kept under lock and key when not in use
- Confidential papers must not be left on desks or in unsecured areas
- Filing cabinets containing personal data are locked when not attended
- Access to areas where personal data is stored is restricted to authorised personnel
- A clear desk policy operates in all areas where personal data is processed
- Visitors are supervised when in areas where personal data may be accessible
- Secure disposal bins are provided for confidential waste
- Keys to secure storage areas are controlled and logged

16.2 Electronic Security

- Strong passwords of at least 10 characters are mandatory for all devices and systems
- Passwords must include a combination of upper and lower case letters, numbers, and special characters where technically possible
- Encryption software is used to protect all portable devices containing personal data
- All school-issued devices have full disk encryption enabled
- Access to electronic systems is protected by appropriate authentication measures
- Regular backups of electronic data are performed and tested (at least termly)
- Backup data is stored securely and separately from live data

- Access to electronic systems is logged and monitored for security purposes

16.3 Cyber Security Measures

The school recognises its direct responsibility to ensure appropriate security protection procedures are in place to safeguard our systems, staff and learners, and to review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies, in accordance with paragraph 144 of Keeping Children Safe in Education 2025.

Our cyber security measures include:
Access Controls

- Multi-factor authentication (MFA) is required for all systems containing personal data
- Strong passwords of at least 10 characters are mandatory for all devices
- Passwords must be changed at least every 90 days
- Access rights are removed immediately when staff leave the school
- Role-based access controls limit data access to only those who need it for their role
- All staff accounts are reviewed termly to ensure access remains appropriate
- Shared accounts are not permitted
- Administrative access is restricted to authorised IT personnel only
- User access is logged and monitored

Technical Safeguards

- Appropriate filtering and monitoring systems are in place and are reviewed at least annually, in accordance with paragraph 139 of Keeping Children Safe in Education 2025
- The school has regard to the DfE's filtering and monitoring standards
- Regular software updates and security patches are applied promptly (within 14 days of release for critical updates)
- Antivirus and anti-malware protection is installed and updated on all devices
- Firewall protection secures the school network
- Secure backup systems are maintained with regular testing of restoration procedures (tested at least termly)
- All portable devices containing personal data are encrypted
- Network segmentation is used where appropriate to limit the spread of potential security incidents
- Intrusion detection and prevention systems are in place where appropriate

Email and Communication Security

- Staff receive regular training on identifying phishing emails and social engineering attempts

- Secure email protocols (TLS encryption) must be used when sharing sensitive information
- Personal email accounts must not be used for school business
- Verification procedures are in place before responding to requests for personal data (e.g., callback verification for telephone requests)
- Suspicious emails must be reported to IT support/DPO immediately
- Email attachments from unknown sources must not be opened
- Links in emails must be verified before clicking
- Spam filtering is in place and regularly updated

Device Security

- All devices containing personal data must be encrypted
- Remote wipe capability is enabled for all school-issued mobile devices
- A clear desk policy operates in all areas where personal data is processed
- Devices must be securely disposed of (with certified data wiping) before disposal or reuse
- Lost or stolen devices must be reported immediately to the DPO and IT support
- Devices must be locked when left unattended (automatic lock after 5 minutes of inactivity)
- Removable media (USB drives, external hard drives) must be encrypted and used only when necessary and approved
- Personal devices used for school work must meet minimum security standards (see Section 16.4)

Compliance with Standards

The school has regard to the following standards and guidance to improve our resilience against cyber-attacks:

- **Cyber Security Standards for Schools and Colleges** (DfE)
- **Keeping Children Safe in Education 2025** (paragraphs 139-148)
- **National Cyber Security Centre (NCSC) guidance**
- **National Education Network guidance on e-security**

We regularly review our compliance with these standards and update our security measures accordingly.

16.4 Remote Access and Personal Devices

Where staff access school systems remotely or use personal devices for school work, the following security measures apply:

16.4.1 Remote Access Requirements

Access must only be via approved secure methods:

- Virtual Private Network (VPN) provided by the school
- Approved cloud services (e.g., Google Workspace for Education)

- Remote desktop services approved by IT support

Security requirements:

- Staff must not access school systems from public or unsecured Wi-Fi networks without using a VPN
- Multi-factor authentication (MFA) is mandatory for all remote access
- Remote access is logged and monitored for security purposes
- Remote access credentials must not be shared with anyone
- Staff must log out of systems when finished
- Devices must not be left unattended while logged into school systems

16.4.2 Personal Devices (BYOD - Bring Your Own Device)

Minimum Security Standards:

Personal devices used for school work must meet the following minimum security standards:

- **Up-to-date operating system** with latest security patches installed
- **Antivirus software** installed, updated, and actively running
- **Screen lock** with password/PIN/biometric authentication enabled
- **Automatic lock** set to activate after maximum 5 minutes of inactivity
- **Encryption** enabled where possible (mandatory for devices storing school data locally)
- **Firewall** enabled and properly configured
- **No jailbreaking/rooting:** Devices must not be jailbroken or rooted
- **Separate user accounts** for school and personal use where technically possible

Data Storage and Handling:

- School data must not be stored locally on personal devices unless:
    - The data is encrypted
    - Prior written approval has been obtained from the DPO
    - The device meets all minimum security standards
- Staff must use approved cloud storage solutions (e.g., Google Workspace) rather than storing data locally on personal devices
- Personal and school data must be kept clearly separated
- School data must not be backed up to personal cloud storage services (e.g., personal iCloud, Dropbox accounts)
- Staff must not sync school data to personal devices via personal accounts

Acceptable Use:

- Personal devices may only be used for approved school purposes
- Staff must comply with all policies, including Acceptable Use Policy, Staff Code of Conduct, and Online Safety Policy
- Personal devices must not be used to access school systems for personal purposes

- Staff must not download or install unauthorised software or apps on devices used to access school systems

Lost or Stolen Devices:

- Staff must report lost or stolen devices immediately to the DPO and IT support (within 2 hours of discovery where possible)
- Personal devices with access to school data may be subject to remote wipe of school data if lost or stolen
- Staff will be informed of this requirement before being granted access to school systems on personal devices
- Staff must sign an acknowledgement that they understand and accept this condition

16.4.3 BYOD Agreement

All staff wishing to use personal devices for school work must:

- Complete a BYOD application form
- Sign a BYOD agreement acknowledging:
    - They understand and will comply with all security requirements
    - They consent to remote wipe of school data if necessary
    - They will report lost/stolen devices immediately
    - They understand the school may inspect the device for compliance purposes
    - They accept responsibility for maintaining the security of their device
- Renew their BYOD agreement annually
- Notify the DPO if their device no longer meets security standards

16.4.4 Device Inspections

The school reserves the right to inspect personal devices used for school work to ensure compliance with this policy. Staff must provide access to their device if requested by IT support or the DPO. Inspections will be conducted with respect for personal privacy, focusing only on school-related data and security settings.

16.4.5 Removal of Access

Access to school systems via personal devices will be immediately revoked when:

- A staff member leaves the school
- A device no longer meets security standards
- There is a suspected security breach
- The BYOD agreement is breached
- The staff member requests removal of access

16.4.6 Compliance and Monitoring

- IT support will conduct periodic audits of personal devices used for school work
- Non-compliance with this policy may result in:

    - Immediate removal of access to school systems
    - Disciplinary action in accordance with the school's disciplinary procedures
- The DPO will maintain a register of all staff using personal devices for school work, including:
    - Staff member name
    - Device type
    - Date BYOD agreement signed
    - Date of last security review
    - Any security incidents

16.5 Incident Response and Business Continuity

We have plans in place to ensure we can limit disruption to teaching and learning if a cyber attack prevents us from accessing our IT systems or data.

Our incident response procedures include:

- Clear roles and responsibilities for the incident response team
- Contact details for key personnel and external support (IT provider, DPO, ICO, NCSC, Action Fraud)
- Steps to contain and mitigate the incident
- Communication procedures for staff, pupils, parents/carers and other stakeholders
- Recovery procedures to restore normal operations
- Review procedures to learn from incidents

These procedures are:

- Documented and kept both electronically (in secure cloud storage) and in hard copy
- Reviewed at least annually
- Tested regularly through simulations
- Updated following any significant incident or change to our IT systems

16.6 Reporting Cyber Security Incidents

All staff must report suspected cyber security incidents immediately to:

- The DPO (dpo@bxs.org.uk)
- IT support
- The Headteacher (for serious incidents)

When a cyber attack occurs, the school will report to:

- **Action Fraud** (0300 123 2040 or www.actionfraud.police.uk) - for all cyber crimes
- **The DfE sector cyber team** (sector.incidentreporting@education.gov.uk) - for all cyber security incidents
- **The National Cyber Security Centre (NCSC)** - if the incident causes long-term school closure, closure of more than one school, or serious financial damage

- **The ICO** (within 72 hours) - where a high risk data breach has or may have occurred
- **Our cyber insurance provider** (if applicable) - in accordance with policy terms

17. Disposal of Records

Personal data that is no longer needed, inaccurate, or out of date will be disposed of securely in accordance with our data retention schedule (Appendix 2) and the principle of storage limitation under Article 5(1)(e) of the UK GDPR.

17.1 Paper Records

Paper-based records containing personal data will be:

- **Shredded** using a cross-cut shredder (minimum DIN P-4 standard for confidential documents)
- **Or incinerated** where appropriate
- **Disposed of by authorised personnel only**
- **Recorded in a disposal log** including:
    - Date of disposal
    - Description of records disposed
    - Method of disposal
    - Name of person authorising disposal
    - Name of person carrying out disposal

Confidential waste bins are provided in appropriate locations and emptied regularly by authorised personnel.

17.2 Electronic Records

Electronic files containing personal data will be:

- **Permanently deleted** (not just moved to recycle bin - files must be deleted from recycle bin/trash)
- **Overwritten** using appropriate data erasure software (e.g., DoD 5220.22-M standard or equivalent) for sensitive data
- **Physically destroyed** if on portable media (e.g., hard drives, USB drives, CDs/DVDs)
- **Certified as destroyed** where appropriate (e.g., for devices containing sensitive data, using a certified IT asset disposal service)
- **Recorded in a disposal log** with similar details as for paper records

Electronic records stored in cloud services (e.g., Google Workspace) will be permanently deleted in accordance with the service provider's deletion procedures.

17.3 Devices

Devices that have stored personal data will be:

- **Securely wiped** using appropriate certified data erasure methods before disposal, reuse, or return
- **Physically destroyed** if secure wiping is not possible (e.g., damaged devices)
- **Disposed of through certified IT asset disposal services** where appropriate
- **Recorded in a disposal log** including:
    - Device type and serial number
    - Date of disposal
    - Method of data erasure/destruction
    - Certificate of destruction (if applicable)
    - Name of person authorising disposal

17.4 Authorisation and Responsibilities

- **Staff must not dispose of any equipment or records that may contain personal data without authorisation from the DPO or IT support**
- Disposal of records must be in accordance with the retention periods specified in Appendix 2
- Any deviation from the retention schedule must be approved by the DPO and documented with justification
- The DPO is responsible for maintaining the disposal log and ensuring disposal procedures are followed
- The School Business Manager is responsible for coordinating the disposal of paper records
- IT support is responsible for the secure disposal of electronic records and devices

17.5 Retention Periods

Personal data will only be retained for as long as necessary to fulfil the purposes for which it was collected, or to comply with legal, regulatory or internal policy requirements.

Our specific retention periods are set out in our Data Retention Schedule (Appendix 2).

When retention periods expire, personal data will be reviewed and:

- Deleted or destroyed if no longer needed
- Retained for a further specified period if there is a legitimate reason (documented and approved by DPO)
- Anonymised if it needs to be retained for statistical or research purposes

18. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes both confirmed and suspected breaches.

In the event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it, in accordance with Article 33 of the UK GDPR.

All staff must be familiar with the data breach procedure and understand their responsibility to report any suspected breach immediately to the DPO.

Examples of data breaches include:

- Loss or theft of devices containing personal data
- Unauthorised access to school systems
- Sending personal data to the wrong recipient
- Cyber attacks such as ransomware or hacking
- Accidental deletion of personal data
- Entering personal data into unauthorised AI tools
- Leaving confidential documents in an unsecured location
- Verbal disclosure of personal information to unauthorised persons
- Unauthorised access to personal data by staff members
- Data sent via insecure methods (e.g., unencrypted email)
- Malware infection leading to data compromise
- Phishing attack resulting in credential theft

19. Training

All members of staff, including supply staff, are required to complete data protection and cyber security training as part of their induction. Refresher training is provided at least annually.

A record of training attendance and completion is kept by the School Business Manager.

19.1 Induction Training (All New Staff)

Before being given access to school systems or personal data, all new staff and supply staff must complete training covering:

- The school's key data protection and security policies
- How to access systems securely
- Who to contact with questions or concerns
- How to report a suspected breach
- Basic cyber security awareness
- The school's acceptable use requirements

19.2 Annual Refresher Training (All Staff)

At least annually, all staff must complete refresher training covering:

Core Data Protection:

- Understanding the UK GDPR and Data Protection Act 2018
- The school's data protection principles and procedures
- How to handle personal data securely
- Subject access requests and individuals' rights
- When and how to report data breaches
- Privacy by design and data minimisation
- The role of the DPO and when to seek advice
- Understanding the difference between data controllers and data processors
- The lawful bases for processing personal data
- Special category data and additional protections required

Cyber Security:

- Recognising and reporting cyber security threats including:
    - Phishing emails and spear-phishing
    - Ransomware attacks
    - Social engineering attempts
    - Malware and viruses
- Safe password practices and multi-factor authentication usage
- Secure handling of personal data in digital formats
- Identifying suspicious emails and communications
- Understanding that AI tools can be used by cyber attackers to create more convincing scam emails
- Incident reporting procedures for suspected cyber attacks
- Safe use of removable media (USB drives, external hard drives)
- Secure remote working practices
- Mobile device security
- Safe internet browsing practices
- Recognising and avoiding common cyber threats

19.3 Role-Specific Training

Staff with specific responsibilities receive additional training:

The DPO receives:

- Specialist data protection and cyber security training
- Attendance at professional development courses and conferences
- Regular updates on changes to legislation and guidance
- Training on conducting DPIAs and managing data breaches

IT staff receive:

- Technical cyber security training
- Training on security technologies and tools
- Updates on emerging threats and security technologies
- Incident response training

Senior leaders receive:

- Training on strategic cyber security management
- Understanding their responsibilities under data protection law
- Training on governance and oversight of data protection
- Business continuity and incident management training

Staff handling sensitive data (e.g., HR, SENCO, Designated Safeguarding Lead) receive:

- Enhanced security training specific to their roles
- Training on handling special category data
- Confidentiality and information sharing training
- Safeguarding-specific data protection training

Governors receive:

- Training on their oversight responsibilities for data protection and cyber security
- Understanding their legal obligations
- How to challenge and support the school on data protection matters
- Understanding data breach reports and risk assessments

19.4 Keeping Training Current

Training is updated regularly to reflect:

- Changes in legislation and guidance
- Emerging cyber threats and attack methods
- Lessons learned from incidents (within our school or nationally)
- New technologies and systems introduced in school
- Feedback from staff on training effectiveness
- Recommendations from the ICO or other regulatory bodies

19.5 Training Delivery Methods

Training may be delivered through:

- Face-to-face sessions during INSET days
- Online modules and e-learning
- Written briefings and updates via email or staff bulletins
- Scenario-based exercises and discussions
- Regular email reminders and tips
- Simulated phishing exercises (with prior notification to staff that these may occur)

19.6 Testing and Assessment

The school may periodically test staff understanding of data protection and cyber security through:

- Short quizzes or assessments
- Simulated phishing exercises
- Scenario-based discussions
- Review of practical application during audits

Results will be used to identify areas where additional training or support is needed, not for disciplinary purposes (unless non-compliance with the policy is identified).

19.7 Training Records

The School Business Manager will maintain records of:

- Training attendance and completion
- Training content delivered
- Assessment results (where applicable)
- Dates of training
- Any follow-up actions required
- Staff members requiring additional support

These records will be reviewed annually by the DPO to identify training needs and gaps.

20. Monitoring Arrangements

The DPO is responsible for monitoring this policy's effectiveness and ensuring compliance with data protection law.

20.1 Annual Review and Audit

The DPO will:

- Conduct an annual audit of data processing activities
- Conduct regular cyber security audits and review security procedures periodically to keep up with evolving cyber-crime technologies, in accordance with paragraph 144 of Keeping Children Safe in Education 2025
- Review filtering and monitoring provision at least annually, in accordance with paragraph 139 of Keeping Children Safe in Education 2025
- Monitor compliance with the Cyber Security Standards for Schools and Colleges
- Review and test backup and recovery procedures (at least termly)
- Assess staff training needs and effectiveness
- Review third-party data processors' security measures
- Evaluate the effectiveness of technical and organisational security measures
- Review the school's compliance with the data protection principles
- Review privacy notices to ensure they remain accurate and up to date
- Review data processing agreements with third parties
- Assess the effectiveness of data protection by design and default measures
- Review the BYOD register and compliance

20.2 Incident Monitoring

The DPO will:

- Maintain a log of all data breaches and security incidents
- Maintain a log of security near-misses and lessons learned
- Monitor trends in security incidents
- Analyse the root causes of incidents
- Identify patterns that may indicate systemic issues
- Review the effectiveness of incident response procedures

20.3 Reporting to the Governing Board

The DPO will provide:

Annual Report to the Governing Board covering:

- Compliance with data protection law
- Summary of data breaches and security incidents
- Training completion rates
- Audit findings and recommendations
- Emerging risks and threats
- Plans for improvement
- Effectiveness of security measures
- Review of third-party processors
- Budget requirements for data protection and cyber security
- Changes to legislation or guidance affecting the school

Quarterly Updates on:

- Significant incidents or changes
- New data processing activities
- Changes to third-party processors
- Training delivered
- Any regulatory correspondence
- Progress on action plans

Immediate Reports on:

- Serious data breaches or security incidents
- Regulatory investigations or enforcement actions
- Significant changes to data protection law
- Major system failures or cyber attacks
- Any incidents reported to the ICO

20.4 Policy Review

This policy will be formally reviewed by the Governing Board every year, or sooner if:

- There are changes to data protection legislation

- There is a significant data breach or security incident
- New technologies or systems are introduced
- The annual audit identifies areas for improvement
- There are changes to the school's data processing activities
- Guidance from the ICO, DfE, or NCSC is updated
- There are changes to the school's organisational structure
- Following recommendations from an inspection or audit

21. Links with Other Policies

This policy is linked to and should be read in conjunction with:

- **Child Protection/Safeguarding Policy** – including online safety and protecting children's data
- **Online Safety Policy** – including filtering, monitoring and cyber security
- **Acceptable Use Agreements** (staff and pupils) – including secure use of technology
- **Staff Code of Conduct** – including data protection responsibilities and professional boundaries
- **Privacy Notices** (pupils, staff, visitors, job applicants) – explaining how we use personal data
- **Records Retention Schedule** (Appendix 2) – how long we keep different categories of data
- **ICT Security Policy** – technical security measures and procedures
- **Bring Your Own Device (BYOD) Policy** – secure use of personal devices for school work
- **Remote Working Policy** – secure remote access procedures
- **Incident Response Plan** – responding to cyber security incidents
- **Business Continuity Plan** – maintaining operations during incidents
- **Behaviour Policy** – including use of CCTV and monitoring of student behaviour
- **Recruitment and Selection Policy** – including safe storage of applicant data
- **CCTV Policy** (if separate) – specific procedures for CCTV operation
- **Social Media Policy** – including protection of personal data online
- **Artificial Intelligence (AI) Policy** – safe and responsible use of AI tools
- **Information Security Policy** – comprehensive security framework
- **Email and Communications Policy** – secure communication practices
- **Freedom of Information Publication Scheme** – proactive publication of information

22. Version Control

Date of Adoption of this Policy	17 December 2025
Date of last review of this policy	November 2024

Date of next review of this policy	October 2026
Policy Owner (SLT)	Hannah Pickles
Policy Owner (Governors)	Adetola Ayenitaju

APPENDICES

Appendix 1: Personal Data Breach Procedure

What is a Personal Data Breach?

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

Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to school systems
- Sending personal data to the wrong recipient
- Cyber attacks such as ransomware or hacking
- Accidental deletion of personal data
- Entering personal data into unauthorised AI tools
- Leaving confidential documents in an unsecured location
- Verbal disclosure of personal information to unauthorised persons
- Unauthorised access to personal data by staff members
- Data sent via insecure methods (e.g., unencrypted email)
- Malware infection leading to data compromise
- Phishing attack resulting in credential theft

Immediate Action (All Staff)

If you discover or suspect a data breach:

1. Act immediately – time is critical in limiting the impact of a breach

2. Contain the breach where possible:

- If a device is lost or stolen, report it immediately so it can be remotely wiped
- If you've sent information to the wrong person, contact them immediately and request deletion (and confirmation of deletion)
- If you suspect a cyber attack, disconnect the affected device from the network (if safe to do so)
- If documents have been left unsecured, secure them immediately
- **Do NOT delete any files or logs** – these are evidence

3. Report immediately to:

- The DPO: dpo@bxs.org.uk
- The Headteacher
- IT support (for technical incidents)

4. Do NOT:

- Discuss the breach with anyone except the DPO, Headteacher, or as directed
- Attempt to "fix" the breach yourself without guidance
- Delete any evidence
- Contact affected individuals directly (the DPO will coordinate this)

Specific Procedures for Cyber Security Incidents

If a cyber attack is suspected (e.g., ransomware, hacking attempt, phishing):

1. Disconnect: Immediately disconnect affected devices from the network (if safe to do so)

- Turn off Wi-Fi and unplug network cables
- Do not turn off the device completely as this may destroy evidence (use sleep/hibernate if possible, or leave strictly isolated)

2. Ransom: Do NOT pay any ransom demands – contact the DPO immediately

- Paying ransoms does not guarantee data recovery
- It may encourage further attacks
- It may be illegal in some circumstances

3. Notify: Contact DPO and IT support immediately

- Provide as much detail as possible about:
    - What you observed
    - When it occurred
    - Which systems or devices are affected
    - Any unusual messages or pop-ups

4. Preserve evidence:

- Do not delete logs, emails or files
- Take photographs of any ransom messages or suspicious activity
- Note the time and circumstances of the incident
- Save any suspicious emails (do not forward them)
- Record any unusual system behaviour

5. Reporting: The DPO/Headteacher will report to:

- **Action Fraud** (0300 123 2040 or www.actionfraud.police.uk)
- **The DfE sector cyber team** (sector.incidentreporting@education.gov.uk)
- **The National Cyber Security Centre (NCSC)** if appropriate
- **The ICO** (within 72 hours) if a high risk data breach has occurred

DPO Actions (Within 72 Hours)

The DPO will:
1. Investigate the Breach

- Establish what happened, when, and how
- Identify what data was involved (type, volume, sensitivity)
- Determine how many individuals are affected
- Assess the risks to individuals (considering the nature of the data and potential consequences)

- Identify measures to contain and recover from the breach
- Determine the root cause
- Assess whether the breach is ongoing

2. Contain and Mitigate

- Take immediate steps to contain the breach
- Implement measures to prevent recurrence
- Coordinate with IT support for technical incidents
- Coordinate with relevant staff to implement containment measures
- Consider whether to involve law enforcement
- Assess whether to inform insurance providers

3. Notify the ICO (within 72 hours of becoming aware) if the breach is likely to result in a risk to individuals' rights and freedoms

This notification will include:

- Nature of the breach
- Categories and approximate number of individuals affected
- Categories and approximate number of personal data records affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate possible adverse effects
- Contact details for further information (DPO contact details)

Note: Not all breaches require ICO notification. The DPO will assess the risk and determine whether notification is required.

4. Notify Affected Individuals (without undue delay) if the breach is likely to result in a high risk to their rights and freedoms

This notification will include:

- Nature of the breach in clear, plain language
- Contact details for further information (DPO contact details)
- Likely consequences of the breach
- Measures taken or proposed to mitigate possible adverse effects
- Advice on steps individuals can take to protect themselves (e.g., changing passwords, monitoring accounts)

5. Document the Breach in the data breach register, including:

- Date and time the breach occurred
- Date and time the breach was discovered
- Facts of the breach (what happened)
- Effects of the breach (actual and potential)

- Personal data involved
- Number of individuals affected
- Categories of data affected
- Remedial action taken
- Whether the ICO and/or individuals were notified
- Lessons learned and preventive measures implemented
- Costs incurred (if significant)

Review and Learning

Following any data breach, the DPO will:

1. Conduct a review to identify:

- Root causes of the breach
- Whether existing controls failed
- What could have prevented the breach
- Lessons learned
- Whether similar breaches could occur elsewhere

2. Update policies and procedures as necessary:

- Revise relevant policies
- Update training materials
- Implement new controls or safeguards
- Update risk assessments

3. Provide additional training to staff if needed:

- Targeted training for those involved
- General awareness training for all staff if systemic issues identified
- Refresher training on specific topics

4. Report to the Governing Board on:

- The incident and its impact
- Actions taken
- Lessons learned
- Recommendations for improvement
- Costs incurred (if significant)
- Changes to policies or procedures

5. Monitor effectiveness of remedial actions

Data Breach Register

The DPO maintains a register of all data breaches, including those not reported to the ICO.

This register includes:

- Date and time of breach
- Description of breach
- Data involved
- Number of individuals affected
- Actions taken
- Whether ICO/individuals were notified
- Outcome and lessons learned
- Preventive measures implemented

This register is:

- Reviewed termly by the Governing Board
- Used to identify trends and systemic issues
- Available for inspection by the ICO
- Kept securely and confidentially

Appendix 2: Data Retention Schedule

The school will only retain personal data for as long as necessary to fulfil the purposes for which it was collected, or to comply with legal, regulatory or internal policy requirements.
Summary of Key Retention Periods

Data Type	Retention Period	Reason/Legal Obligation	Disposal Method
Pupil Records (Educational Record)	6 years after the pupil leaves the school	To satisfy administrative needs and defence of legal claims	Secure shredding (paper) / Secure deletion (electronic)

Pupil Special Educational Needs (SEN) Records	35 years after the pupil leaves the school	To satisfy potential future requests or claims relating to educational needs	Secure shredding (paper) / Secure deletion (electronic)
Child Protection/Safeguarding Records	Until the subject reaches age 25, or 6 years after leaving (whichever is later)	Statutory requirement under Keeping Children Safe in Education (KCSIE)	Secure shredding (paper) / Secure deletion (electronic). Transfer to new school where appropriate
Pupil Attendance Records	Current year + 3 years	For statutory returns and potential legal claims	Secure shredding (paper) / Secure deletion (electronic)
Pupil Medical Records	Current year + 6 years (or until age 25 if longer)	To satisfy potential legal claims and duty of care	Secure shredding (paper) / Secure deletion (electronic)
Admission Registers	Current year + 6 years	Legal requirement and potential legal claims	Secure shredding (paper) / Secure deletion (electronic)

Staff HR Records (successful applicants)	6 years after the employee leaves the school	To comply with tax, employment law, and defence against legal claims	Secure shredding (paper) / Secure deletion (electronic)
Staff HR Records (unsuccessful applicants)	6 months after recruitment process concludes	To defend against potential discrimination claims	Secure shredding (paper) / Secure deletion (electronic)
Staff Personnel Files	6 years after employment ends	Employment law and defence against legal claims	Secure shredding (paper) / Secure deletion (electronic)
DBS Certificates (copies)	Maximum 6 months after recruitment decision	Data protection compliance (should not be retained longer than necessary)	Secure shredding (paper) / Secure deletion (electronic)
Accident/Incident Reports (pupils)	DOB of pupil + 25 years	Potential legal claims	Secure shredding (paper) / Secure deletion (electronic)

Accident/Incident Reports (staff/visitors)	Date of incident + 6 years	Potential legal claims	Secure shredding (paper) / Secure deletion (electronic)
CCTV Footage	Maximum of 30 days	Monitoring and security purposes. Longer retention only if required for investigation	Automatic overwriting / Secure deletion
Financial Records (invoices, receipts, etc.)	Current year + 6 years	Tax and audit requirements	Secure shredding (paper) / Secure deletion (electronic)
Payroll Records	Current year + 6 years	Tax and employment law requirements	Secure shredding (paper) / Secure deletion (electronic)
Governor Meeting Minutes	Permanent (or current year + 10 years minimum)	Historical record and governance accountability	Archive securely
Email Correspondence (general)	Review and delete regularly	Data minimisation principle	Secure deletion

	(suggested: 2 years)		
Email Correspondence (significant)	Retain as per subject matter (e.g., if relates to safeguarding, follow safeguarding retention)	Depends on content	Secure deletion
Website Analytics	Maximum 26 months	Privacy and data protection compliance	Automatic deletion
Photographs/Videos (with consent)	While consent remains valid and purpose remains relevant	Consent-based processing	Secure deletion when consent withdrawn or no longer needed
Data Breach Records	Indefinitely (or minimum 7 years)	Accountability and regulatory compliance	Secure storage
DPIA Records	For the life of the processing activity + 6 years	Accountability and regulatory compliance	Secure deletion
Data Processing Agreements	Duration of contract + 6 years	Legal and regulatory compliance	Secure deletion

Notes:

-

Sources:

Keeping Children Safe in Education
Keeping Children Safe in Education