



BARHAM CHURCH OF ENGLAND PRIMARY SCHOOL

DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

Kind, confident and curious

Document control

Item	Detail
Policy owner	Governing Body
Senior Responsible Person	Headteacher
Data Protection Officer	Satswana Ltd
DPO email	admin@satswana.com
School contact	office@barham.kent.sch.uk
School address	Valley Road, Barham, Canterbury, Kent, CT4 6NX
School ICO registration	Z7592934
Version	2.0 - governor review draft
Reviewed	July 2026
Approved	8.10.26
Review date	September 2027

Approved by the governing body:	Date: October 2026
Next scheduled review:	September 2027

Earlier review required if:	law, statutory guidance, school processing or DPO advice changes materially
-----------------------------	---

Governor review summary

The May 2026 policy contained several material points requiring correction or expansion. The substantive changes in this draft are:

- Correction of the Data (Use and Access) Act 2025 description. School holidays do not create a general pause or extension for subject access requests.
- Retention periods corrected for a primary school. The main pupil record transfers when the pupil leaves; it is not routinely retained by the primary school until age 25. Child protection records are retained to age 25, with records relating to child sexual abuse retained to age 75.
- A complete subject access request process, parental educational record process and Freedom of Information/Environmental Information process have been added.
- The new statutory data protection complaints process has been added, including acknowledgement within 30 days and response without undue delay.
- Breach reporting thresholds have been clarified: report to the ICO within 72 hours where a breach is likely to risk people's rights and freedoms, and inform affected people without undue delay where the risk is high.
- Provisions on photographs, recordings, CCTV, AI, EdTech, personal devices, cyber security and automated decision-making have been made clearer and more proportionate.
- Incorrect or duplicated school and DPO contact details, the school name typo, and several drafting errors have been corrected.

DPO confirmation recommended: Because Satswana Ltd is the school's appointed DPO and supplied the May 2026 template, the governing body should ask Satswana to confirm this redline before formal adoption, particularly the contact details and the school's separate retention schedule.

Contents

1. Policy statement and scope
 2. Definitions
 3. Legal framework and guidance
 4. Data controller and accountability
 5. Roles and responsibilities
 6. Data protection principles
 7. Lawful processing
 8. Special category and criminal offence data
 9. Privacy information and children
 10. Sharing personal data and international transfers
 11. Individual rights and subject access requests
 12. Parental access to educational records
 13. Photographs, videos and recordings
 14. CCTV and biometric data
 15. Artificial intelligence, EdTech and automated decisions
 16. Data protection by design and DPIAs
 17. Information security and personal devices
 18. Retention, archiving and secure disposal
 19. Personal data breaches
 20. Training and awareness
 21. Data protection complaints
 22. Freedom of Information and Environmental Information
 23. Monitoring and review
- Appendix A - Personal data breach response procedure

Appendix B - Information request handling checklist

Appendix C - Key legal and guidance references

1. Policy statement and scope

We protect the data and information we hold about every person as the law requires.

Barham Church of England Primary School is committed to protecting the privacy, dignity and rights of pupils, parents and carers, staff, governors, volunteers, visitors and all other people whose personal data we process.

This policy applies to personal data held in any format, including electronic systems, email, messaging tools, paper files, photographs, video, audio, CCTV and information held by service providers on the school's behalf.

Where processing concerns a child, the child's best interests are a primary consideration. This does not remove the legal rights of other data subjects; decisions will be lawful, fair, proportionate and made case by case.

This policy applies to all members of the workforce, governors, volunteers, contractors and organisations processing personal data on behalf of the school. Failure to follow it may lead to disciplinary, contractual or other appropriate action.

2. Definitions

Term	Meaning
Controller	The person or organisation that decides why and how personal data is processed. Barham CE Primary School is the controller for processing it determines. Other bodies, such as Kent County Council or the Department for Education, may be separate controllers for their own statutory processing.
Data subject	An identified or identifiable living person whose personal data is held or used.
Personal data	Information relating to an identified or identifiable living person.
Processing	Anything done with personal data, including collecting, recording, organising, storing, changing, retrieving, consulting, using, sharing, restricting, erasing or destroying it.
Special category data	More sensitive personal data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric identification data, health, sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences, allegations or related security measures.
Processor	A person or organisation that processes personal data on behalf of a controller under a written contract.
Personal data breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
DPIA	A Data Protection Impact Assessment used to identify and reduce risks before high-risk processing begins or changes materially.
SAR	A subject access request made by a person, or by someone authorised to act for them, for access to their personal data and related information.
FOI request	A written request for recorded information under the Freedom of

Term	Meaning
	Information Act 2000.
EIR request	A request for environmental information under the Environmental Information Regulations 2004. It may be verbal or written.
Retention schedule	The school's approved rules for how long different records are retained, reviewed, transferred, archived and securely destroyed.
Pseudonymisation	Replacing direct identifiers with a code while keeping the additional identifying information separately and securely.
Anonymisation	Irreversibly removing the ability to identify a person so that the information is no longer personal data.

3. Legal framework and guidance

This policy is based on and should be read with the following legislation and statutory requirements:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025, which amends rather than replaces the UK GDPR and Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Education (Pupil Information) (England) Regulations 2005
- Privacy and Electronic Communications Regulations 2003, where applicable
- Protection of Freedoms Act 2012, including the use of biometric data and surveillance camera systems
- Computer Misuse Act 1990
- Human Rights Act 1998 and Equality Act 2010
- Children Act 1989, Children and Families Act 2014 and relevant safeguarding law and guidance

The school will have regard to current guidance from the Department for Education (DfE) and the Information Commissioner's Office (ICO), including guidance on data protection in schools, records management, photographs and CCTV, generative AI, EdTech procurement and cyber security.

The Data (Use and Access) Act 2025 introduced changes including reasonable and proportionate searches for SARs, limited circumstances in which the response clock may be paused for reasonable clarification, recognised legitimate interests, safeguards for significant automated decisions and statutory complaint-handling duties. It does not allow schools to extend SAR deadlines merely because of school holidays.

4. Data controller and accountability

The school processes personal data about pupils, parents and carers, staff, governors, applicants, volunteers, visitors and others. It is registered with the ICO and pays the data protection fee where required.

The governing body is accountable for ensuring that the school complies with data protection and information rights law. The Headteacher is the Senior Responsible Person and acts for the controller on a day-to-day basis. Operational tasks may be delegated, but accountability remains with the governing body and Headteacher.

The school will maintain appropriate accountability records, including privacy notices, a record of processing activities, processor and supplier records, DPIAs, consent records where consent is relied on, information request logs, training records and a breach log.

5. Roles and responsibilities

5.1 Governing body

- ensures appropriate policies, procedures, resources and oversight are in place;

- receives appropriate assurance and at least an annual report on data protection compliance;
- approves this policy and monitors material risks and actions.

5.2 Data Protection Officer

- provides independent advice on the school's data protection obligations;
- monitors compliance, training, audits and DPIAs;
- is consulted promptly about breaches, high-risk processing, complex rights requests, contracts, international transfers and new technologies;
- acts as a contact point for data subjects and the ICO and reports directly to the highest management level.

5.3 Headteacher / Senior Responsible Person

- oversees day-to-day implementation and ensures staff follow this policy;
- appoints any Delegated Lead in writing and defines responsibilities and escalation routes;
- ensures information rights requests, complaints and breaches are logged and handled within legal timescales;
- ensures data protection is considered in school improvement, procurement, safeguarding, curriculum and operational decisions.

5.4 All workforce members, governors and volunteers

- only access and use personal data needed for authorised school duties;
- follow approved systems, security controls, privacy notices and retention rules;
- keep personal data accurate and report changes to their own details;
- recognise that a rights request may be verbal, written or contained within a complaint and pass it immediately to the Headteacher or DPO;
- report any actual or suspected breach immediately and do not investigate, delete evidence or contact affected people without instruction;
- seek advice before introducing new technology, sharing data outside routine arrangements or using personal data for a new purpose.

6. Data protection principles

Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed securely, with protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

The school must also be able to demonstrate compliance with these principles (the accountability principle).

7. Lawful processing

The school will identify and document at least one lawful basis before processing personal data. The lawful bases are:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task or official authority;
- recognised legitimate interests;
- legitimate interests.

For most core educational, safeguarding and statutory functions, the school will usually rely on public task or legal obligation rather than consent. Consent will only be used where a genuine choice can be offered and withdrawal will not cause unfair detriment.

The school will not rely on ordinary legitimate interests for processing undertaken as part of its public-authority tasks. It may rely on legitimate interests or recognised legitimate interests for appropriate non-public-task processing, after documenting necessity and any required safeguards.

Where the school wishes to use personal data for a new purpose, it will consider compatibility with the original purpose, identify a lawful basis, update privacy information and obtain consent where the law requires it.

8. Special category and criminal offence data

The school will only process special category data where it has both an Article 6 lawful basis and an Article 9 condition. Common conditions include employment and social protection law, substantial public interest, health or social care, public health, vital interests, legal claims and explicit consent where appropriate.

Criminal offence data will only be processed where the school has an Article 6 lawful basis and an applicable condition or legal authority under the Data Protection Act 2018. The school will maintain an appropriate policy document where required.

Access to special category and criminal offence data will be restricted to people who need it for authorised duties, with enhanced security and retention controls.

9. Privacy information and children

When the school collects personal data directly, it will provide clear privacy information explaining how and why the data is used, lawful bases, sharing, retention, rights and how to complain. Where data is obtained from another source, the school will provide the information required by law unless an exemption applies.

Privacy notices will be concise, accessible and written in language appropriate to the intended audience. Where online services are likely to be accessed by children, their needs and vulnerabilities will be taken into account in design and procurement.

Children have their own data protection rights. Capacity and understanding will be considered individually; age is a guide, not an absolute rule.

10. Sharing personal data and international transfers

The school will share personal data only where there is a lawful basis, a clear and necessary purpose, and proportionate security. It will share the minimum information required and keep an appropriate record of significant or non-routine sharing decisions.

Consent is not normally required where information must be shared to safeguard a child, comply with law, carry out a public task or protect vital interests. Safeguarding information will be shared promptly with appropriate agencies when necessary, with the DSL involved and the decision recorded.

Before sharing with suppliers or processors, the school will complete proportionate due diligence, ensure a compliant written contract is in place, confirm sub-processors and data locations, and check deletion/return arrangements at the end of the service.

When a pupil moves to another school, the school will transfer the common transfer file, educational record and safeguarding information securely and traceably within the required timeframe. Safeguarding files will be transferred separately and confirmation of receipt obtained.

Personal data will only be transferred outside the UK where an adequacy regulation or other lawful transfer mechanism and any required supplementary safeguards are in place. The DPO will be consulted before a new international transfer begins.

11. Individual rights and subject access requests

Depending on the circumstances, individuals may have rights of access, rectification, erasure, restriction, objection, data portability, withdrawal of consent and safeguards relating to automated decision-making. Requests must be passed immediately to the Headteacher or DPO.

11.1 Recognising and receiving a SAR

- A SAR can be made verbally or in writing, including by email, letter, telephone, social media or within a complaint. The requester does not need to use the words “subject access request”.
- Any member of staff or volunteer may receive a SAR. They must record the date and wording accurately and forward it immediately.
- The school may offer a form to help clarify a request but cannot require the requester to use it or restart the request in another format.
- Identity, parental responsibility or authority to act may be checked only to the extent reasonably necessary.

11.2 Response time and searches

- The school will respond without undue delay and normally within one calendar month.
- The response period begins when the school has the request and any information reasonably required to confirm identity. The clock may be paused where reasonable clarification is genuinely required, until clarification is received.
- For a complex request, or where the same person has made several requests, the period may be extended by up to two further months. The requester will be told within the first month, with reasons and the revised deadline.
- School holidays do not, by themselves, pause or extend the statutory deadline.
- The school will carry out reasonable and proportionate searches of relevant systems and records, including paper files, email, messages, CCTV and information held by processors where applicable.

11.3 Responding, exemptions and fees

- Information will normally be provided free of charge, securely and in a clear, accessible format.
- The school may charge a reasonable fee for additional copies or, where legally permitted, a manifestly unfounded or excessive request.
- Third-party personal data will be redacted unless it is reasonable to disclose it without consent. Any exemption will be applied case by case, documented and explained as far as the law permits.
- If the school refuses all or part of a request, it will explain the reason, the right to complain to the school and the right to complain to the ICO or seek a judicial remedy.

11.4 Requests by or for children

A child does not have to reach a particular age to make a SAR. The school will assess the child's maturity and understanding. Where a child can understand and exercise the right, the response will normally be made to the child. A parent may act for a child where the child authorises this or lacks sufficient understanding, subject to the child's best interests and safeguarding considerations.

For primary-age pupils, it will often be appropriate to deal with a parent's request on the child's behalf, but this is not automatic. The school will consider the child's views, confidentiality, family circumstances, safeguarding risks and any court orders case by case.

12. Parental access to educational records

This section applies to the maintained-school right of a person with parental responsibility to access a pupil's educational record under the Education (Pupil Information) (England) Regulations 2005. This is separate from the child's and parent's rights under data protection law.

- A written request to inspect or obtain a copy of the educational record will be handled within 15 school days.
- Inspection is free. The school may charge no more than the cost of supplying a copy.
- Information may be withheld where a legal exception applies, including where disclosure would be likely to cause serious harm to the physical or mental health of the pupil or another person, reveal protected third-party information, or disclose exam marks before official publication.
- Where a request overlaps with a SAR, the school will identify and apply the correct legal regime and explain this to the requester.

13. Photographs, videos and recordings

The school may take photographs, video or audio recordings for teaching, assessment, celebration, safeguarding, security and communication. The purpose, lawful basis, expected audience, retention and security will be considered before use.

13.1 School use

- Images used only within routine teaching, assessment or internal records may be processed under public task or another appropriate lawful basis, as explained in the relevant privacy notice.
- The school will obtain specific, recorded permission where it relies on consent, particularly for identifiable use in public-facing marketing, promotional publications or social media. Refusing or withdrawing consent will not disadvantage the pupil.
- Where an alternative lawful basis is relied on, the school will provide a clear opt-out and respect objections unless it has compelling lawful grounds to continue.
- The school will avoid publishing a pupil's full name with an image unless there is a clear need and appropriate permission or lawful basis.
- When permission is withdrawn or an objection is upheld, the school will stop future use and remove content from websites, social media or other channels it controls where reasonably practicable. It may not be possible to recall printed material already distributed or copies controlled by third parties.

13.2 Images taken by parents and carers

Personal photographs and videos taken by parents or carers for domestic use are generally outside data protection law. The school may restrict recording at an event where necessary for safeguarding, privacy, copyright, performance licensing or the safe and orderly running of the event. Images of other children must not be posted publicly without appropriate permission.

13.3 Meetings and other recordings

No person may record a meeting, telephone call, lesson or conversation involving the school without prior agreement, unless they have a lawful right to do so. Requests to record as a reasonable adjustment or accessibility aid will be considered case by case under the Equality Act 2010. Where the school records for a lawful purpose, participants will normally be told in advance and the recording will be secured, access-controlled and retained only as long as necessary.

14. CCTV and biometric data

14.1 CCTV

The school uses CCTV at the main office entrance for security and safeguarding. It will display appropriate signage, maintain a clear purpose and lawful basis, restrict access, set a proportionate retention period and respond to access requests in line with data protection law. CCTV will not be used for a new purpose without review and, where required, a DPIA.

14.2 Biometric data

The school does not currently use an automated biometric recognition system. Before introducing one, it would complete a DPIA, consult the DPO, provide alternatives and obtain the written consent required by the Protection of Freedoms Act 2012. A pupil's objection must be respected even where parental consent has been given.

15. Artificial intelligence, EdTech and automated decisions

15.1 AI and generative AI

- Only school-approved AI tools and accounts may be used for school business.
- Personal, confidential, safeguarding, special category or criminal offence data must not be entered into an AI tool unless the use has been specifically approved, the lawful basis and contract are clear, privacy and training settings have been checked, and any required DPIA has been completed.
- Staff must minimise or anonymise data before using AI wherever possible and must not use pupil work, names, images, reports or case information to train public models.

- AI outputs must be checked by a competent human for accuracy, bias, safeguarding, copyright, confidentiality and appropriateness before use.
- An unapproved disclosure of personal data to an AI service will be treated as a potential personal data breach and reported immediately.

15.2 EdTech procurement

Before acquiring or materially changing educational technology, the school will assess necessity, age appropriateness, accessibility, privacy information, lawful basis, data minimisation, profiling, advertising, security, data location, sub-processors, retention/deletion, exit arrangements and supplier assurance. The DPO and IT representative will be consulted according to risk.

15.3 Automated decision-making

The school will not make a legally or similarly significant decision about a pupil, parent or member of staff solely by automated processing without a lawful basis and appropriate safeguards. Safeguards will include meaningful information, the ability to make representations, human intervention and a route to contest the decision. Extra restrictions apply where special category data is used.

16. Data protection by design and DPIAs

Data protection will be considered from the beginning of a project and throughout its life. The school will apply data minimisation, clear access controls, secure defaults, appropriate retention, transparent information and privacy-friendly settings.

A DPIA will be completed before processing likely to result in a high risk to people, including certain uses of monitoring, CCTV, biometrics, AI, profiling, large-scale special category data, systematic sharing or new technology. The DPO's advice will be recorded. Processing will not begin while an unmitigated high risk remains without the required consultation.

The school will maintain a processor list and proportionate supplier assurance. Low-risk technology must still be approved through the school's procurement and IT processes; listing a product does not replace due diligence or a compliant contract.

17. Information security and personal devices

The school will use proportionate technical and organisational measures to protect confidentiality, integrity and availability. Measures include access based on role and need, encryption, secure backups, patching, anti-malware, filtering and monitoring, secure configuration, physical security and tested incident response.

17.1 Accounts, passwords and access

- Use a strong, unique password or passphrase for each school account and never share it.
- Use multi-factor authentication where available or required by the school.
- Lock devices when unattended and sign out of shared systems.
- Do not use personal email, unauthorised cloud storage or consumer messaging services for school personal data.
- Access must be removed or changed promptly when roles change or people leave.

17.2 Portable media and personal devices

School personal data must not be stored on a personal device unless the Headteacher and IT representative have explicitly authorised the arrangement and appropriate management, encryption, access, backup, deletion and incident controls are in place. Removable media must be school-approved and encrypted. Personal data taken off site must be necessary, minimised and protected.

17.3 Email and secure sharing

- Check recipients and attachments before sending, use BCC appropriately and avoid auto-complete errors.
- Use approved encrypted or secure transfer methods for sensitive information.
- Do not send passwords in the same message or channel as protected files.
- Report misdirected messages immediately; do not rely on recall or deletion alone.

18. Retention, archiving and secure disposal

The school will maintain and follow a detailed retention schedule. Records will be retained only for as long as there is a legal, safeguarding, operational, historical or evidential need. An annual personal data audit will identify records to retain, transfer, anonymise or destroy.

18.1 Key pupil-record rules

- The main primary-school pupil record is retained until the pupil leaves and is then transferred securely to the next school. Core MIS data is normally kept for two terms after the pupil leaves to meet census and transfer needs.
- Child protection files are transferred separately and securely to the new school. The retention endpoint is the child's 25th birthday; records relating to child sexual abuse are retained until the child's 75th birthday.
- There is no blanket statutory rule requiring a primary school to keep all SEND records, routine educational records or records of looked-after children until age 25 or 75. Retention will follow the record's content, applicable law, safeguarding need and the approved schedule.
- Where litigation, an investigation, safeguarding need or other legal hold applies, relevant destruction will be suspended and the decision documented.

18.2 Disposal and backups

- Paper records will be cross-cut shredded or destroyed by an approved confidential-waste contractor.
- Electronic records and storage media will be securely erased or destroyed so that the data cannot reasonably be reconstructed.
- Destruction will be authorised by an appropriate senior leader and documented, including a description, date, method and authoriser. Certificates of destruction will be retained where a contractor is used.
- Backup copies may persist until overwritten through the normal backup cycle. They will remain protected, will not be restored for routine use after the retention endpoint, and will be deleted or rendered inaccessible in line with the schedule.

19. Personal data breaches

All actual or suspected personal data breaches must be reported immediately to the Headteacher, DPO and relevant IT or safeguarding lead. The school will follow Appendix A and will not wait for complete information before escalating.

The school will contain the incident, preserve evidence, assess the likelihood and severity of risk to people, document the facts and decisions, and take remedial action. Every breach will be logged, including breaches not reported externally.

Where a breach is likely to result in a risk to people's rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. Where the risk is high, affected people will also be informed without undue delay unless a legal exception applies.

Safeguarding concerns will be addressed immediately in parallel with the data protection response. Law enforcement, insurers, the local authority, cyber response bodies or other partners may be contacted where appropriate.

20. Training and awareness

Staff, governors and relevant volunteers will receive appropriate data protection and cyber security training at induction and regular refresher training. Additional role-based training will be provided for those handling safeguarding records, information requests, HR, finance, IT, procurement, communications and high-risk data.

Training completion will be recorded. Lessons from incidents, audits, complaints, near misses and changes in law or technology will be communicated promptly.

21. Data protection complaints

A person who believes the school has not complied with data protection law can complain by contacting the school office or the DPO. The school will provide a clear electronic route for complaints and reasonable assistance where needed.

- School contact: office@barham.kent.sch.uk
- DPO: Satswana Ltd - admin@satswana.com
- The school will acknowledge a data protection complaint within 30 days.
- It will investigate appropriately, keep the complainant informed where necessary and communicate the outcome without undue delay.
- The response will explain any action taken and the right to complain to the Information Commissioner's Office.

Complaints about teaching, behaviour, admissions or other school matters that do not concern personal data will be handled under the school's Complaints Policy. A complaint may engage both procedures, in which case the school will coordinate them and preserve the applicable legal timescales.

22. Freedom of Information and Environmental Information

The school is a public authority for the purposes of the Freedom of Information Act 2000 and will adopt and publish the ICO model publication scheme, a guide to information and an appropriate fees schedule.

22.1 Valid requests and assistance

- An FOI request must be in writing, give the requester's real name and an address for correspondence, and describe the recorded information requested.
- A request for environmental information may be made verbally or in writing and will be handled under the Environmental Information Regulations 2004.
- The school will provide reasonable advice and assistance and may seek clarification where needed to identify and locate the information.

22.2 Time limits and responses

- The school will respond promptly and, for FOI requests, within 20 school days or 60 working days, whichever is sooner, subject to any lawful extension.
- The response will confirm whether the information is held, disclose it in the requested form where reasonably practicable, or issue a written refusal notice explaining the exemption or other reason relied on.
- Personal data will be considered under data protection law and the applicable FOI exemption; a person seeking their own personal data will normally be directed to the SAR process.
- The school may charge only where the law, regulations or published fees schedule permits. It may refuse a request that exceeds the statutory cost limit, while giving advice and assistance where appropriate.

22.3 Review and complaint

A requester may ask the school for an internal review. The review will be carried out by someone appropriately independent of the original decision and will normally be completed within 20 working days, or as soon as reasonably practicable where complexity requires longer. The outcome will explain the right to complain to the ICO.

23. Monitoring and review

The DPO and Headteacher will monitor this policy and related procedures. Compliance will be reviewed through audits, breach and request logs, training records, supplier reviews, DPIAs, complaints and the annual data audit.

The governing body will review and approve the policy at least annually and sooner if there is a material change in law, statutory guidance, school systems, processing activities, safeguarding practice or DPO advice.

Appendix A - Personal data breach response procedure

1. Report immediately - Tell the Headteacher/DPO at once. Include what happened, when, systems or records involved, people affected, whether data is still exposed and any safeguarding concern. Do not delay because facts are incomplete.

2. Contain and recover - Take proportionate steps to stop further loss or access: recall or disable links, contact the unintended recipient, reset credentials, isolate devices, preserve logs and evidence, and involve IT or safeguarding leads.

3. Record the incident - Open a breach log entry with time of discovery, time the school became aware, data and people affected, containment, decisions, communications and actions.

4. Assess risk - Consider the nature, sensitivity and volume of data; ease of identification; people's vulnerability; likely consequences; number affected; and whether security measures such as encryption reduce risk.

5. Decide on ICO notification - Notify the ICO without undue delay and, where feasible, within 72 hours where the breach is likely to risk people's rights and freedoms. If reporting later, explain the delay. Record reasons where no notification is made.

6. Inform affected people - Where the breach is likely to create a high risk, communicate without undue delay in clear language, describing the breach, likely consequences, action taken, protective steps and DPO contact details, unless a legal exception applies.

7. Coordinate other notifications - Consider safeguarding partners, police, local authority, insurer, cyber response support, banks, suppliers or others according to the incident. Keep communications accurate and controlled.

8. Review and improve - Identify root cause, complete remedial actions, update risk assessments, contracts, systems, training or procedures, and report significant incidents and lessons to governors.

Appendix B - Information request handling checklist

B1. Subject access requests

- Log the exact date, method and wording; notify the Headteacher/DPO immediately.
- Confirm identity/authority only where reasonably necessary; record any pause for clarification.
- Calculate one calendar month; do not exclude school holidays.
- Map reasonable and proportionate searches, including processors and relevant messages/CCTV.
- Preserve originals; redact securely and check redactions cannot be reversed.
- Apply exemptions case by case; document reasons and DPO advice.
- Send securely with privacy information, rights and complaint route; retain an audit copy.

B2. FOI/EIR requests

- Decide whether the request is FOI, EIR, SAR or a combination.
- Log the request and calculate the correct statutory deadline.
- Clarify scope where needed and provide advice and assistance.
- Search for recorded information held at the time of the request, including by contractors on the school's behalf.
- Consider cost limits, personal data and other exemptions/exceptions; apply the public-interest test where required.
- Issue the information or a compliant refusal notice; explain internal review and ICO rights.
- Publish frequently requested information proactively where appropriate.

Appendix C - Key legal and guidance references

- UK General Data Protection Regulation and Data Protection Act 2018
- Data (Use and Access) Act 2025
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Education (Pupil Information) (England) Regulations 2005
- Department for Education: Data protection in schools (updated 9 July 2026)
- Department for Education: Meeting digital and technology standards in schools and colleges
- Information Commissioner's Office: UK GDPR, subject access, data sharing, breaches, complaints, CCTV, FOI and publication scheme guidance
- Keeping Children Safe in Education and Working Together to Safeguard Children
- Protection of Freedoms Act 2012 and Surveillance Camera Code where applicable
- School policies and procedures on safeguarding, acceptable use, cyber security, records retention, complaints, staff conduct, photography/online safety and business continuity.

Approved by the governing body:	Date:
Chair of Governors signature:	Headteacher signature:
Next scheduled review:	July 2027
Earlier review required if:	law, statutory guidance, school processing or DPO advice changes materially