St Annes College Grammar School



Data Protection Policy

Policy owner	St Annes College Ltd, registered proprietor and data controller
Responsible lead	Principal, Abigail Welsby
Data protection officer	Head of PD/ICT
Approved by	St Annes College Ltd; 27th September 2026
Policy date	September 2026
Effective from	27th September 2026
Review date	September 2027 or sooner after a material change

This policy explains how St Annes College Grammar School handles personal information about pupils, families, staff and others. It also tells staff how to share information to safeguard children, respond to requests and report a suspected breach. It must be read with the safeguarding and child protection policy, privacy notices, retention schedule and relevant operational procedures.

1 Scope and legal framework

This policy applies to all staff, directors, Advisory Body members, volunteers, contractors and others who handle personal data for the school, whether on paper, in school systems or elsewhere. The school complies with the UK General Data Protection Regulation, Data Protection Act 2018 and applicable changes made by the Data (Use and Access) Act 2025. It has regard to Keeping Children Safe in Education 2026 (KCSIE), Working Together to Safeguard Children, statutory information sharing guidance and guidance of the Information Commissioner's Office (ICO).

2 Controller and responsibilities

St Annes College Ltd is the registered proprietor of SACGS and is responsible for the school's data protection governance. The company is the data controller for school processing carried out in its name. It determines purposes and means of processing, ensures suitable policies and resources, and receives material risk and breach reports. The Advisory Body provides advice and scrutiny under its terms of reference; it is not a governing body or a substitute for the proprietor's legal accountability.

The Data Protection Officer leads implementation, and escalates significant decision to the Principal for authorisation. The designated safeguarding lead (DSL), directs safeguarding decisions, referrals and transfers of child protection records. Staff must report concerns promptly and follow the DSL's direction; an absent DSL must never delay an urgent referral.

The school's data protection officer (DPO) is contactable through the school office. The proprietor ensures that the DPO has appropriate expertise, independence, resources and direct access to the highest management level. The DPO advises, monitors compliance, assists with DPIAs and is a contact point for individuals and the ICO. She does not decide the purposes or means of the processing for which she provides independent oversight. Staff must send requests and incidents to the DPO immediately. Because the DPO also has ICT responsibilities, the Principal must document and manage any conflict of interest: she advises and monitors independently, while the Principal makes decisions about the purposes and means of processing, selection and configuration of systems, access permissions and breach notification. Where a matter concerns the DPO's own operational work, the proprietor obtains independent advice or review and records the decision.

All staff must use personal data only for authorised work, keep it secure and accurate, complete training, and report concerns, requests and suspected breaches immediately. Contractors processing data for the school must follow written instructions and contractual security requirements.

3 Principles and lawful processing

We process personal data lawfully, fairly and transparently; collect it for specified purposes; limit it to what is necessary; keep it accurate; retain it no longer than necessary; protect it appropriately; and demonstrate accountability. Privacy notices explain the categories, purposes, lawful bases, recipients, retention, rights and contact route. Staff must not assume that consent is the lawful basis for routine education or safeguarding processing. The appropriate Article 6 basis and, where relevant, an Article 9 special-category condition or Article 10 and Schedule 1 condition for criminal-offence data must be identified and recorded for each purpose. Public task is used only where the school can identify an applicable function in law; its independent status alone does not establish that basis.

Health, SEND, safeguarding, biometric and other sensitive information receives additional safeguards. Data is collected directly where practicable, checked and corrected where needed, and accessed only by those with a legitimate need. Corrections to records must preserve any legally required audit history, including admission and attendance records.

4 Safeguarding information sharing

Data protection law permits proportionate information sharing to safeguard children. Staff must pass a concern to the DSL without delay and record what was seen, heard, shared and decided. If a child is in immediate danger, staff must contact emergency services or children's social care as appropriate and then inform the DSL. A staff member may make a referral directly if necessary; they must not wait for consent or for an unavailable colleague.

The DSL decides what relevant information should be shared with children's social care, police, safeguarding partners, health professionals, a receiving school or another appropriate body. Consent is not invariably required and must not be sought where it could put a child at risk, impede an investigation or cause harmful delay. The DSL considers the lawful basis, necessity, proportionality, the child's interests, confidentiality and any applicable restriction, and records the rationale, recipient, secure method and date. When appropriate, the child and parents are told what has been shared, unless doing so would create risk or prejudice protection work.

Child protection files are kept separately from the general pupil record with controlled access. On a school transfer, the DSL arranges secure, timely transfer to the receiving DSL, confirms receipt and considers whether relevant information should be shared in advance so support is in place. The school retains a transfer record. Safeguarding records are retained in accordance with the retention schedule and any legal hold; staff must not delete them simply because a pupil leaves.

The September 2026 statutory information sharing guidance will be followed. The duty under section 16LA of the Children Act 2004 commences on 30 September 2026. From that date, the DSL and proprietor will apply it where the school, recipient, purpose and information fall within its scope; staff continue to share information lawfully to protect children before commencement.

5 Other sharing and processors

We share information with local authorities, examination bodies, health and education partners, regulators, law enforcement and service providers where a lawful basis permits or requires it. We provide the minimum necessary through an appropriate secure channel and record unusual or sensitive disclosures. Routine sharing arrangements are documented where appropriate. Processors, including MIS and IT suppliers, must have suitable contracts, access controls and security assurances. International transfers require an applicable UK transfer mechanism and risk assessment where required. Before introducing a new supplier or significant information sharing arrangement, the Principal and DPO review the purpose, lawful basis, processor or controller roles, security, contractual terms, retention and any international transfer. Where the processing is likely to pose high risk, the school completes a DPIA before it begins and records the residual risk and decision.

6 Individual rights and requests

A subject access request (SAR) may be made verbally or in writing and need not mention the UK GDPR. Staff must send it immediately to the DPO. We verify identity only to the extent reasonably necessary, locate and review records, apply exemptions individually, protect third-party information and respond within the statutory period, normally one month. A permitted extension for complex or numerous requests must be explained within that first month. We do not demand two forms of identification as a blanket rule.

A child's own rights and understanding are assessed individually. There is no fixed age at which parental access automatically starts or ends. Parental responsibility does not itself give an unconditional right to every item of a child's personal data. We consider the child's competence, wishes, welfare, any court order and relevant exemptions. Separate rules on access to an educational record are considered where applicable to this independent school; we do not promise a route that law does not provide. Requests for rectification, erasure, restriction, objection, portability or withdrawal of consent are assessed according to the applicable right and lawful basis. A refusal is explained with the right to complain to the ICO.

7 Images CCTV and biometric information

Photography and video for marketing or publication use a clearly explained permission process, with separate choices where appropriate. We respect pupil views and safeguarding restrictions; withdrawal stops future use and prompts removal where reasonably practicable, but cannot always retrieve material already lawfully distributed. Internal educational images are handled under the relevant lawful basis and privacy notice. Families are asked to respect the privacy of other children when sharing event images.

CCTV is used for documented safety and security purposes with visible notices, restricted access, a retention period set by the CCTV schedule (normally 30 days unless preserved for a specific matter) and controlled disclosure. Cameras are not placed in toilets, changing rooms or shower areas. A camera covering a treatment or welfare space requires a specific necessity and privacy assessment before installation. Any change of purpose or unusually intrusive installation requires prior assessment.

8 AI and new technology

Staff must use only AI tools authorised by the Principal for school work and follow the approved conditions for each tool. Identifiable pupil, safeguarding, medical, SEND and personnel data may be entered only where the school has established a lawful purpose, approved supplier terms and security, completed a data protection impact assessment (DPIA) where required, and specified access, retention and human checking. De-identification must be effective in context. Outputs must be checked by a competent member of staff; decisions about pupils are made by authorised people, with appropriate safeguards for any automated decision making. Suspected entry into an unauthorised tool is reported immediately as a possible breach, not automatically classified as a reportable breach. The approved tool register identifies permitted purposes, users, categories of data, safeguards and review date. Staff may use identifiable information for an authorised purpose only within the tool and conditions expressly approved for it; a personal subscription or apparent anonymisation is not approval.

9 Security retention and disposal

Access is role based and reviewed when duties change or employment ends. Staff use approved accounts, strong authentication, encryption and secure transfer methods; they avoid personal devices or accounts unless expressly approved with controls. Paper records are secured, screens locked, and portable information minimised and protected. Suppliers and systems are reviewed for suitable controls, backups and recovery. Staff report loss, misdirection, unauthorised access or system compromise immediately.

Records are retained according to the school's approved retention schedule, safeguarding requirements, legal duties and any investigation or litigation hold. Destruction must be secure and documented where appropriate. No staff member may erase a safeguarding record or alter an audit trail to respond to a request.

10 Breaches and complaints

Anyone who suspects a personal data breach must immediately contact the DPO and the Principal through the school office; where safeguarding information may be affected, they must also notify the DSL without delay. The school contains the incident, preserves evidence, assesses the likelihood and severity of harm, records its reasoning and tells the proprietor of material incidents. The controller reports a breach to the ICO within 72 hours of becoming aware of it when it is likely to result in a risk to individuals' rights and freedoms; if the risk is high, affected individuals are informed without undue delay unless an exception applies. The DPO advises but the controller remains accountable. Appendix 1 gives the response steps.

Privacy concerns may be raised through the school office for the DPO and Principal. Individuals may complain to the ICO. Safeguarding concerns follow the safeguarding policy even if they also involve personal data.

11 Training monitoring and review

Staff receive role-appropriate induction and refreshers. The Principal monitors compliance, incident patterns and completion of actions with the DPO and DSL. The proprietor approves this policy and reviews it at least annually or sooner after legal, technical or organisational changes. The school reviews its records of processing, privacy notices, retention schedule, supplier contracts and data protection risks at least annually. The DPO provides independent advice to the proprietor; the Principal records and owns the actions arising.

Source documents

Keeping Children Safe in Education 2026, Department for Education, September 2026; Information sharing to safeguard children and young people, Department for Education, September 2026; UK GDPR and Data Protection Act 2018 as amended; ICO guidance on sharing information to safeguard children and personal data breaches.