ST DOMINIC'S GRAMMAR SCHOOL

DATA PROTECTION AND UK GDPR POLICY

Academic Year 2026–2027

Safeguarding priority. Data protection law does not prevent necessary and proportionate information sharing to protect a child. Immediate risk must be reported to the DSL without delay.

Policy control	Approved position
Applies to	Whole School: Nursery and EYFS to Sixth Form; staff, governors, volunteers, contractors and relevant visitors
Policy owner	Headmaster
Operational lead	Sharon Tillett, Operational Data Protection Lead – stillett@sdgschool.co.uk
Proprietor	Mr Gary Hartland
Approval date	30 August 2026
Effective date	1 September 2026
Next review	By 31 August 2027, or earlier following material legal, regulatory, safeguarding or technological change
Publication	Staff SharePoint; relevant public information on the School website

Status of lead. The School has determined that it is not required to appoint a statutory Data Protection Officer. Sharon Tillett is the operational Data Protection Lead and must not be described as the data controller or statutory DPO. The Proprietor retains legal accountability.

1. Purpose and application

This policy explains how St Dominic's Grammar School complies with the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 (DUAA) and associated law. It applies to personal data in every format and system, not only electronic information, and to all School activities from Nursery and EYFS to Sixth Form.

It applies to prospective, current and former pupils and parents; staff, applicants and former staff; governors, volunteers and contractors; visitors, alumni, donors, suppliers and other individuals whose personal data the School processes. Compliance is a condition of access to School information and systems; deliberate or reckless breach may result in disciplinary, contractual or legal action.

2. Legal and regulatory framework

- UK General Data Protection Regulation, as amended.
- Data Protection Act 2018.
- Data (Use and Access) Act 2025, including amendments in force from 2026.
- Privacy and Electronic Communications Regulations 2003.
- Human Rights Act 1998 and Equality Act 2010.
- Education, safeguarding, employment, health and safety, pupil registration, examination, taxation and regulatory duties.
- DfE data protection in schools guidance, updated 9 July 2026; ICO guidance; current Independent School Standards and ISI expectations.

3. Controller and governance

The data controller is St Dominic's Grammar School, Bargate Street, Brewood, South Staffordshire, ST19 9BA, acting through its Proprietor, Mr Gary Hartland.

The School is not required to appoint a statutory DPO. Sharon Tillett is the Operational Data Protection Lead and can be contacted at stillet@sdgschool.co.uk or through the School office on 01902 850248. She coordinates compliance, advice, records, rights requests, breaches, DPIAs, complaints and training, but does not replace the accountability of the Proprietor, Headmaster, system owners or every person handling data.

Role	Responsibilities
Proprietor	Ultimate accountability; approves policy and risk appetite; receives assurance; ensures resources; challenges and tracks high-risk action.
Governing Body	Delegated scrutiny, support and challenge; reviews anonymised trends, audit and action completion.
Headmaster	Implements policy; assigns owners; ensures training, secure systems, procurement controls and incident response.
Operational Data Protection Lead	Advises and coordinates; maintains accountability records; manages requests, breaches, DPIAs and complaints; escalates material risk.
Network Manager/system owners	Apply access, security, backup, logging, deletion and supplier controls; preserve evidence and report incidents.
DSL	Leads safeguarding decisions and ensures data-protection considerations do not obstruct lawful child protection.
All personnel	Use data only as authorised; maintain confidentiality and accuracy; report errors, requests, risks and breaches immediately.

4. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person, including opinions and online identifiers.
Special-category data	Data revealing racial or ethnic origin, political opinions, religious/philosophical beliefs, trade-union membership, genetic or biometric identification, health, sex life or sexual orientation.
Criminal-offence data	Information about criminal allegations, proceedings, convictions, offences or related security measures.
Processing	Any operation involving personal data, including collection, recording, use, sharing, storage, alteration, retrieval, deletion or destruction.
Controller	The person or organisation that determines the purposes and means of processing.
Processor	A separate organisation processing personal data on the controller's documented instructions.
Data subject	The living individual to whom personal data relates.
Personal data breach	Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. 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 no longer than necessary;
- protected by appropriate technical and organisational security; and
- handled with demonstrable accountability.

6. Accountability framework

The School maintains and reviews an evidence set proportionate to its processing and risks:

- Record of Processing Activities/information asset register, including purposes, categories, recipients, transfers, retention and security;
- lawful-basis schedule, Article 9/10 conditions and any required appropriate policy document;
- current privacy notices and consent records where consent is genuinely relied upon;
- Records Retention Schedule, deletion records and legal holds;
- processor, data-sharing, EdTech and international-transfer registers;
- DPIA screening decisions, completed DPIAs and privacy-by-design actions;
- rights-request, complaint, breach and near-miss logs;
- training, audit, governance challenge, decisions and corrective-action records.

7. Lawful bases and purpose limitation

Before processing begins, the School identifies and records the purpose and an Article 6 lawful basis. It does not retrospectively select a convenient basis or assume that all educational processing has the same basis.

Basis	School application
Contract	Necessary to enter into or perform a contract with the individual, including relevant parent or employment arrangements.
Legal obligation	Necessary to comply with education, safeguarding, employment, taxation, health and safety or regulatory law.
Vital interests	Exceptional processing needed to protect life where another basis is unavailable.
Public task	Used only where a specific task in the public interest or official authority has a clear basis in law; it is not assumed for all independent-school activity.
Legitimate interests	A genuine interest, necessity and balancing of individual rights are documented; an LIA is completed where appropriate.
Recognised legitimate interests	Used only where the statutory DUAA category and conditions apply; not a blanket replacement for assessment.
Consent	Freely given, specific, informed and unambiguous; evidenced and withdrawable without detriment. Not used where imbalance or another basis makes it inappropriate.

New use of existing data is assessed for compatibility or supported by a new lawful basis and transparency. The DUAA provisions are applied only where in force and relevant, with the decision documented.

8. Special-category and criminal-offence data

An Article 6 basis alone is insufficient. The School records the applicable Article 9 condition for special-category data and the relevant Data Protection Act 2018 basis/safeguard for criminal-offence data. Explicit consent is not the default: safeguarding, employment, health, equality, legal claims or substantial public-interest conditions may be more appropriate. Where required, an Appropriate Policy Document is maintained.

9. Privacy, transparency and children

- Privacy information is concise, accessible and provided at or before collection, or within the statutory period when obtained elsewhere.
- Separate notices are maintained as appropriate for parents/pupils, workforce, recruitment, CCTV/visitors, alumni/fundraising and website services.
- Notices identify controller/contact details, data and sources, purposes and bases, recipients, transfers, retention, rights, complaints and material automated decision-making.
- Children's competence, wishes, best interests and confidentiality are considered. Parents do not automatically own a child's personal data or rights.
- Where transparency would create a safeguarding risk, information is limited only where law permits and reasoning is recorded.
- Consent for an online service offered directly to a child follows the applicable UK age and parental-authorisation rules; ordinary school processing is not assumed to rely on consent.

10. Collection, quality and records

- Collect the minimum necessary data and avoid speculative or excessive recording.
- Records must be factual, professional, relevant and intelligible; opinions are identified as such.
- Reasonable steps are taken to verify important data and correct inaccuracies without undue delay.
- Individuals and staff must notify relevant changes; disputed accuracy is marked while assessed.
- Unofficial duplicate records, local spreadsheets and uncontrolled email archives are avoided.
- Information asset owners review their data, permissions, retention and continuing necessity at least annually.

11. Security and confidentiality

- Role-based least-privilege access, periodic reviews and prompt leaver/change removal.
- Strong unique passwords, multi-factor authentication where available, encryption, screen locking and secure configuration.
- Approved School email, storage, devices, transfer and disposal; no unapproved personal email, cloud storage, removable media or public AI.
- Clear desk/screen, secure printing, locked storage, recipient and permission checks and appropriate Bcc use.
- Secure backup, restoration testing, logging, patching, malware protection and incident/continuity planning.
- Paper or electronic data taken off site only where authorised, necessary and protected in transit and storage.
- Confidentiality continues after employment, study, governorship or contract ends.

12. Information sharing and safeguarding

Child protection. Consent is not required where another lawful basis permits necessary and proportionate safeguarding sharing. Staff record what was shared, with whom, why and any decision not to share; urgent protection is never delayed by seeking routine data-protection approval.

- Verify identity, authority, recipient and purpose; share the minimum necessary through an approved secure route.
- Routine recipients may include local authorities, DfE, regulators/inspectors, exam boards, UCAS, other education providers, health and safeguarding partners, police, insurers, advisers and approved suppliers where lawful.
- Police, court and regulator requests are verified and referred to the Data Protection Lead unless emergency action is required.
- Separated-family and portal access decisions consider parental responsibility, court orders, competence, safety, confidentiality and third-party rights; fee payment alone does not confer access.
- Safeguarding records transfer separately and securely under safeguarding procedures.
- Data-sharing agreements are used where scale, sensitivity, recurrence or joint working warrants them.

13. Processors, EdTech and procurement

No app, platform, plugin, AI system, cloud service or supplier may process School personal data until authorised procurement and data-protection checks are completed. Staff acceptance of free online terms is not approval.

- Confirm controller/processor roles, purpose, lawful basis, minimum data and age appropriateness.
- Assess supplier competence, security, accessibility, sub-processors, data location, retention/training use, breach support, audit, exit, deletion and data return.
- Put Article 28 terms in place for processors and document controller-to-controller arrangements.
- Screen for a DPIA and international-transfer requirements before commitment.
- Record owner, review/renewal date and exit plan; export/delete data when use ends.
- Ensure monitoring information is restricted to authorised trained staff and connected to clear safeguarding and retention procedures.

14. Data protection by design and DPIAs

Privacy and security are built into the design of projects and defaults. A DPIA is mandatory before processing likely to result in high risk, including systematic monitoring, new biometric/facial recognition, large-scale sensitive data, innovative AI/profiling or significant automated decisions.

- Project owner completes screening before procurement, pilot or material change.

- The DPIA describes nature, scope, context and purposes; assesses necessity and proportionality; identifies risks; and records mitigations, owner and residual risk.
- The Data Protection Lead advises and records whether a DPIA is unnecessary. Relevant stakeholders and, where appropriate, affected people are consulted.
- High residual risk that cannot be mitigated is escalated and prior ICO consultation considered before processing starts.
- The DPIA is reviewed when risk, system, purpose, supplier or data changes.

15. International transfers

Personal data is transferred outside the UK only under a valid adequacy regulation, UK International Data Transfer Agreement/addendum, binding corporate rules, permitted derogation or another lawful mechanism. A required data-protection test/transfer risk assessment and supplementary safeguards are documented. Supplier assurances alone are insufficient.

16. Retention, archiving and disposal

- The approved Records Retention Schedule governs pupil, safeguarding, SEND, medical, examination, HR, finance, governance, CCTV, visitor, IT and incident records in every format.
- Owners review holdings at least annually and configure systems for defensible deletion where possible.
- Safeguarding, legal, insurance and limitation needs are reflected; active disputes, investigations or legal holds suspend routine deletion.
- At expiry, information is securely destroyed, deleted or irreversibly anonymised and material destruction is evidenced.
- Backups are protected and expire through controlled rotation; they are not used as indefinite archives.

17. Individual rights

Depending on the circumstances, individuals may have rights to be informed, access, correction, erasure, restriction, objection, portability, withdrawal of consent and safeguards in relation to qualifying automated decisions. Rights are not absolute and exemptions are applied narrowly, case by case, with recorded reasoning.

- Any oral or written rights request is forwarded immediately to Sharon Tillett, regardless of whether it mentions GDPR.
- Identity and third-party authority are verified proportionately; unnecessary copies of identity documents are avoided.
- The School responds without undue delay and normally within one month, subject to lawful clarification, extension, fee, refusal or exemption.
- Searches are reasonable and proportionate across relevant MIS, email, drives, paper, safeguarding, HR, archived and supplier systems.
- Third-party information, safeguarding risk, privilege, negotiations and other exemptions are assessed; redaction is used where appropriate.
- A child's own competence, wishes and best interests are considered. A parental request is not automatically treated as the child's request.
- Decisions, searches, redactions, disclosures and a secure response copy are retained under the schedule.

18. Automated decision-making and AI

- Personal or confidential data is not entered into public or unapproved AI services.
- Approved use requires lawful basis, transparency, data minimisation, processor and transfer checks, security, accuracy/bias assessment, retention/training-use review and DPIA screening.
- Solely automated decisions producing legal or similarly significant effects are used only where lawful, with required information, safeguards, meaningful human involvement and a route to contest.
- Human reviewers must have genuine authority and competence, not merely endorse an automated output.

- Material AI processing is reflected in the ROPA and relevant privacy notice.

19. Direct marketing, images, CCTV and biometrics

- Electronic marketing complies with PECR and data-protection law; consent or another permitted route is recorded, preferences are honoured and opt-out is simple.
- Pupil images are used under a documented purpose and basis, with minimum identification and additional assessment for sensitive/high-profile uses.
- CCTV has defined purposes, signage/privacy information, access controls, retention and disclosure procedures and a separate policy where appropriate.
- Biometric recognition requires specific legal compliance, necessity and proportionality assessment, DPIA, transparency and any consent or alternative arrangements required by law.
- Facial recognition and covert monitoring are not introduced without explicit Proprietor approval, specialist advice and documented legal assessment.

20. Personal data breaches

Stage	Action
Report immediately	Tell Sharon Tillett and relevant IT/system owner; make safe; do not conceal error, forward sensitive material unnecessarily or delete evidence.
Contain and preserve	Restrict access, recall messages if possible, reset credentials, isolate equipment where advised and preserve logs/evidence.
Assess	Record nature, cause, people and data affected, sensitivity/volume, likely consequences and existing safeguards; DSL assesses child risk.
Notify ICO	Where risk to rights and freedoms is likely, the controller notifies without undue delay and, where feasible, within 72 hours of awareness; delay and non-notification reasons are recorded.
Inform individuals	Where high risk is likely, communicate without undue delay unless a lawful exception applies; provide practical protective advice.
Learn	Complete the breach log, consider insurer/police/NCSC/other bodies, review controls and training and report material learning to governance.

21. Complaints

A person may complain orally or in writing to Sharon Tillett at stillet@sdgschool.co.uk or through the School office. The School acknowledges and investigates objectively without undue delay, provides an outcome and any remedy, keeps a central log and offers reasonable adjustments. The person whose work is challenged is not the sole decision-maker. The complainant is informed of the right to complain to the Information Commissioner's Office at ico.org.uk or 0303 123 1113.

22. Training, monitoring and assurance

- All staff receive induction and regular refreshers appropriate to their access and role; governors and specialist staff receive role-specific training.
- Training covers secure handling, sharing, safeguarding, breaches, rights requests, phishing, EdTech/AI and reporting routes; attendance and follow-up are recorded.
- The Data Protection Lead conducts or coordinates proportionate audits and tracks corrective actions.

- At least annually the Headmaster presents assurance to the Proprietor/Governing Body covering ROPA and notices, lawful bases, retention, rights, breaches, complaints, DPIAs, processors, transfers, training, security, incidents and overdue/high-risk actions.
- The policy is reviewed annually and after significant law, guidance, processing, technology, ownership or incident change.

Appendix 1 – Immediate staff rules

- Use only information you are authorised to access and only for the approved School purpose.
- Use approved systems, devices, storage and communication routes.
- Check recipients, attachments, permissions and sensitivity before sharing.
- Keep records accurate, factual, relevant and secure.
- Do not disclose credentials, leave screens unlocked, access records out of curiosity or use unapproved AI/cloud services.
- Report suspected breaches and near misses immediately; do not conceal mistakes.
- Forward every rights request, correction request or data complaint immediately to Sharon Tillett.
- Ask before starting a new form, spreadsheet, app, survey, monitoring process or supplier that collects personal data.
- Share safeguarding information when necessary and proportionate; report immediate child risk to the DSL without delay.

Appendix 2 – DPIA screening questions

Before a new or materially changed project begins, the owner records whether it involves:

- new technology, AI, profiling or automated decisions;
- systematic or large-scale monitoring;
- biometric, genetic, health, safeguarding, SEND, equality or criminal-offence data;
- large numbers of children or vulnerable people;
- matching datasets, location tracking, behavioural analysis or novel use;
- denial of a service, opportunity, access or significant benefit;
- new suppliers, sub-processors, international transfers or opaque terms;
- processing that could create physical, financial, reputational, discriminatory, confidentiality or safeguarding harm.

If any answer indicates likely high risk or uncertainty, contact Sharon Tillett and do not proceed until the screening decision and any DPIA are approved and recorded.

Appendix 3 – Subject access action checklist

1. Record receipt immediately and send to Sharon Tillett.
2. Confirm request scope, identity and any representative's authority proportionately.
3. Identify systems, custodians, suppliers and date ranges; preserve relevant data.
4. Conduct reasonable and proportionate searches and record search instructions/results.
5. Review for the requester's personal data, accuracy, third parties, safeguarding, privilege and exemptions.
6. Redact securely; quality-check completeness, attachments, metadata and recipient.
7. Provide the response securely with required supplementary information within the legal period.
8. Record decisions, correspondence, disclosure and complaints; retain the response copy under the schedule.

Appendix 4 – Annual assurance checklist

- Controller/ICO registration and lead contact details verified.
- ROPA, asset owners, lawful bases and privacy notices reviewed.
- Retention schedule applied and overdue deletion/legal holds checked.
- Processors, EdTech, contracts, transfers and exit plans reviewed.
- DPIA screening and high-risk actions reviewed.
- Rights requests, complaints, breaches and near misses analysed for timeliness and trends.
- Access reviews, leavers, security testing, backup/restore and incident arrangements evidenced.
- Training completion and understanding checked.

- Material risks, overdue actions and decisions reported to the Proprietor/Governing Body and tracked to closure.

Appendix 5 – Authoritative sources

- UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025.
- DfE, Data protection in schools, updated 9 July 2026.
- ICO guidance on accountability, lawful bases, children, individual rights, security, breaches, DPIAs and international transfers.
- Keeping Children Safe in Education 2026 and current information-sharing guidance.
- Current Independent School Standards guidance and ISI framework and handbook.