DATA PROTECTION AND PRIVACY POLICY

Policy Owner:	Chief Operating Officer (COO)
ISSR Reference:	Part 3 - Welfare, Health and Safety of Pupils Part 8 - Quality of Leadership in and Management of Schools
Date of review:	Summer 2026
Approved by:	Group Board
Date of next review	Summer 2027

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Tier 1 policy formatted into SDEG house style and running order	Chief Operating Officer (COO)	Group Board – Summer 2026	Streamlined format, monitoring wording and policy links aligned to house style

1. Aims

This is the principal Tier 1 policy for personal data across SDEG. It is supported by the Photography, Filming & Image Use Policy, Data Incident & Breach Response Protocol and the SDEG Statutory Privacy Notices.

SDEG processes personal information to educate and safeguard pupils, employ and support staff, govern and operate its schools and nurseries, communicate with families and communities, meet legal obligations and pursue its charitable purposes. This Policy establishes the Group-wide principles, governance, responsibilities and minimum controls for doing so lawfully, fairly, transparently and securely.

It applies to personal data in electronic, paper, image, audio, video and other formats, whether processed directly by SDEG or by a processor acting on its behalf. It is non-contractual, but breach may lead to disciplinary, safeguarding, contractual or governance action.

1.1 Core principles

Principle	Application
Lawfulness, fairness and transparency	Use a valid lawful basis, treat people fairly and explain processing clearly.
Purpose limitation	Collect and use data for specified, explicit and legitimate purposes.
Data minimisation	Use only data that is adequate, relevant and necessary.
Accuracy	Keep data accurate and rectify material errors without avoidable delay.
Storage limitation	Retain identifiable data only for as long as necessary.
Integrity and confidentiality	Protect data with appropriate technical and organisational measures.
Accountability	Document decisions, ownership, controls, risks and assurance.
Privacy by design and default	Consider privacy at the outset and use privacy-protective defaults.
Children's interests	Give particular regard to the rights, understanding and vulnerability of children.
Human accountability	Significant decisions remain subject to meaningful human oversight.

2. Legislation and Regulatory Framework

- UK General Data Protection Regulation;
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003;
- Freedom of Information Act 2000 where applicable;

- Education Act 1996, Children Acts and other education and safeguarding legislation;
- Human Rights Act 1998;
- Equality Act 2010; and
- current ICO and Department for Education guidance.

SDEG will monitor regulatory guidance as reforms are implemented. From 19 June 2026 controllers must maintain a process for data-protection complaints; SDEG therefore incorporates complaint handling within this Policy and its privacy notices.

2.1 Definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living individual.
Special-category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership; genetic data; biometric data used for identification; health data; or information concerning a person's sex life or sexual orientation.
Criminal-offence data	Personal data relating to criminal convictions and offences, allegations, proceedings, Disclosure and Barring Service checks and related security or safeguarding measures.
Data subject	The living individual to whom personal data relates.
Controller	The organisation that determines why and how personal data is processed. For this Policy, the controller is St Dunstan's Education Group.
Processor	A person or organisation that processes personal data on behalf of the controller.
Processing	Any operation performed on personal data, including collecting, recording, organising, storing, changing, retrieving, using, sharing, disclosing, restricting, deleting, destroying or anonymising it.
Consent	A freely given, specific, informed and unambiguous indication of an individual's wishes, given by a clear statement or affirmative action.
DPIA	A Data Protection Impact Assessment used to identify, assess and reduce privacy risks in proposed or changed processing.

DPO	The Data Protection Officer, who provides independent advice and monitors compliance with data-protection law.
ICO	The Information Commissioner's Office, the UK supervisory authority for data protection.
ROPA	The Record of Processing Activities maintained to document SDEG's processing and demonstrate accountability.
UK GDPR	The United Kingdom General Data Protection Regulation.
PECR	The Privacy and Electronic Communications Regulations 2003.

3. Roles and responsibilities

3.1 Group Board of Governors

- approve this Policy and retain ultimate oversight as the governing body of the controller;
- hold the COO to account for implementation, capability and assurance;
- receive annual assurance on rights requests, complaints, breaches, DPIAs, audits, training, suppliers and improvement; and
- receive prompt escalation of material incidents or risks.

3.2 Chief Operating Officer and Group DPO

- own this Policy and act as executive owner for data protection;
- oversee day-to-day compliance and represent the controller;
- provide or commission independent advice and external support from Judicium;
- maintain routes for rights requests, complaints and breach reporting;
- advise on high-risk processing, data sharing, contracts, DPIAs and retention;
- report to the CEO and Group Board; and
- maintain appropriate independence when discharging DPO responsibilities and escalate any conflict.

3.3 Contacting the Data Protection Officer

Questions about this Policy, concerns about the use of personal data, rights requests and data-protection complaints may be directed to the Chief Operating Officer or to SDEG's external Data Protection Officer service:

Data Protection Officer: Judicium Consulting Limited Address: 5th Floor, 98 Theobalds Road, London WC1X 8WB
Email: dataservices@judicium.com
Website: www.judiciumeducation.co.uk
Telephone: 0345 548 7000

The DPO provides independent advice and may be contacted directly where an individual considers this appropriate. Contacting SDEG or the DPO does not affect an individual's right to complain to the ICO.

3.4 CEO, Heads and Directors

The CEO ensures the COO has appropriate authority and resources. Heads and Directors are accountable for compliant processing in their schools and functions, including records, systems, staff practice, suppliers, privacy information, adjustments and action closure.

3.5 Director of Digital Services

The Director of Digital Services operates technical security, identity, access, backup, logging, incident and supplier controls under the Digital Services, Information Security & Cyber Resilience Policy and supports DPIAs, rights requests and breach response.

3.6 All staff and authorised users

- access personal data only where authorised and necessary;
- use approved systems and follow handling requirements;
- keep information accurate and secure;
- complete mandatory training;
- recognise and report rights requests, complaints and incidents immediately; and
- seek advice before new, changed, unusual or high-risk processing.

4. Data protection and privacy framework

4.1 Lawful processing

Every processing activity must have a documented purpose and lawful basis. SDEG will only process personal data where at least one lawful basis under Article 6 UK GDPR applies. The basis selected must reflect the actual purpose and circumstances of the processing and must be reviewed if those circumstances change.

4.2 Article 6 lawful bases

- Consent: the individual has given clear permission for processing for a specific purpose.
- Contract: processing is necessary to perform a contract with the individual or to take steps at the individual's request before entering into a contract.
- Legal obligation: processing is necessary to comply with a legal duty.
- Vital interests: processing is necessary to protect someone's life.
- Public task: processing is necessary to perform a task in the public interest or an official function that has a clear basis in law.
- Legitimate interests: processing is necessary for SDEG's or a third party's legitimate interests, unless the individual's interests, rights or freedoms override those interests.

Consent will be used only where it is freely given, specific, informed and unambiguous. It must be as easy to withdraw as to give. SDEG will retain evidence of consent and will stop the consent-based processing when consent is withdrawn unless another lawful basis applies.

4.3 Special-category data and Article 9 conditions

Special-category data requires both an Article 6 lawful basis and an additional condition under Article 9 UK GDPR. Where required by the Data Protection Act 2018, SDEG will also identify the relevant Schedule 1 condition and maintain an appropriate policy document.

Depending on the activity, the Article 9 conditions relied upon by SDEG may include:

- explicit consent;
- employment, social-security and social-protection law;
- protection of vital interests where the individual is unable to consent;
- personal data manifestly made public by the individual;
- the establishment, exercise or defence of legal claims;
- substantial public interest, including safeguarding and equality-related purposes where the statutory conditions apply;
- preventive or occupational medicine, assessment of working capacity, medical diagnosis, or provision or management of health or social care;
- public interest in the area of public health; and
- archiving in the public interest, scientific or historical research, or statistical purposes where the legal requirements and safeguards apply.

SDEG will apply appropriate safeguards, data minimisation, access restrictions, confidentiality and retention controls whenever special-category data is processed.

4.4 Criminal-offence and criminal-records data

SDEG may process information relating to criminal convictions and offences, allegations, proceedings, Disclosure and Barring Service checks, safeguarding concerns and related suitability or security measures where permitted by law.

Such processing must have an Article 6 lawful basis and must either be carried out under official authority or satisfy an applicable condition in Schedule 1 of the Data Protection Act 2018. The condition, necessity, proportionality and safeguards must be documented.

Access will be restricted to authorised people with a legitimate need to know. DBS certificate information and criminal-record information will not be retained for longer than permitted by law and the Group Data Retention Schedule.

4.5 Records of Processing Activities

SDEG will maintain a Record of Processing Activities showing the purposes of processing, categories of people and data, lawful bases and additional conditions, recipients, locations,

retention periods, international transfers, security measures and accountable owners. Heads and Directors must ensure that material changes in their areas are reflected in the ROPA.

4.6 Transparency and privacy notices

SDEG will provide clear, accessible and age-appropriate privacy information when personal data is collected and, where required, when it is obtained indirectly. The SDEG Statutory Privacy Notices consolidate notices for pupils and families, staff, applicants, governors and volunteers, and visitors and contractors. Significant new processing will trigger review and update.

4.7 Data subject rights and complaints

Individuals have rights under UK GDPR. The availability of a right depends on the circumstances and lawful basis, and exemptions may apply. SDEG will explain any lawful restriction or refusal.

4.8 Right to be informed

Individuals are entitled to clear information about how and why their personal data is used, normally through privacy notices and just-in-time information.

4.9 Right of access

Individuals may ask whether SDEG processes their personal data and request a copy together with supplementary information about the processing.

4.10 Right to rectification

Individuals may ask for inaccurate personal data to be corrected and incomplete information to be completed.

4.11 Right to erasure

Individuals may ask for personal data to be deleted where the legal conditions apply. This is not an absolute right and may not apply where retention is required by law, safeguarding duties, legal claims or another lawful reason.

4.12 Right to restriction

Individuals may ask SDEG to limit the use of their personal data in specified circumstances, for example while accuracy or an objection is considered.

4.13 Right to object

Individuals may object to processing based on public task or legitimate interests. SDEG will consider the objection and whether compelling lawful grounds require the processing to continue. The right to object to direct marketing is absolute.

4.14 Right to data portability

Where processing is automated and based on consent or contract, individuals may in applicable cases request personal data they provided in a structured, commonly used and machine-readable format or ask for it to be transmitted to another controller where technically feasible.

4.15 Rights relating to automated decisions

Individuals may have the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects, and may request human intervention, express a view and challenge the decision.

4.16 Right to withdraw consent

Where consent is relied upon, it may be withdrawn at any time. Withdrawal does not affect processing carried out lawfully before withdrawal.

4.17 Right to complain

Individuals may complain to SDEG and may also complain to the ICO.

4.18 Exercising rights

A request does not need to refer to UK GDPR or use a particular form. It may be made verbally or in writing and should be forwarded immediately to the Chief Operating Officer. SDEG may verify identity and authority proportionately and may seek clarification where necessary. The normal response period is one calendar month, subject to lawful provisions relating to clarification, extension, fees or refusal.

Requests concerning children will be handled in accordance with section 8. SDEG will keep a central record of requests, searches, decisions, disclosures and response dates.

4.19 Data-protection complaints

Complaints may be made through any reasonable channel and will be routed to the Chief Operating Officer. SDEG will acknowledge receipt within 30 days, investigate without undue delay, keep the complainant appropriately informed and communicate the outcome without undue delay. People will be told of their right to complain to the ICO.

4.20 Direct marketing and fundraising communications

Where SDEG undertakes direct marketing, promotional communications, fundraising communications or alumni engagement, it will comply with UK GDPR and PECR. SDEG will identify the appropriate lawful basis and obtain consent for electronic marketing where PECR requires it.

Individuals will be given clear and accessible choices and may object or unsubscribe at any time. An objection to direct marketing is absolute and will be acted upon promptly and free of charge. Suppression information may be retained to ensure that the individual is not contacted again through the objected-to channel. Marketing data will not be used in a way that is inconsistent with the relevant privacy information.

4.21 Children and parental requests

Rights belong to the child. When a request is made by or on behalf of a child, SDEG will consider maturity, understanding, parental responsibility, confidentiality, safeguarding, court orders, the child's views and potential detriment. Information will not be released merely because an adult has parental responsibility where disclosure would be inappropriate or unlawful.

4.22 Privacy by design, DPIAs and change

A DPIA is required where processing is likely to result in high risk, including relevant use of new technology, systematic monitoring, profiling, solely automated significant decisions, large-scale special-category data or other high-risk uses. The assessment will describe processing and purpose, test necessity and proportionality, assess risks to people and record mitigations, consultation and approval.

No significant new system, supplier, integration, AI use, monitoring activity or changed use of personal information should proceed until privacy, safeguarding, security, contractual and retention questions have been addressed.

4.23 Sharing, processors and international transfers

- share only where necessary, lawful, proportionate and consistent with privacy information;
- verify identity, authority, purpose and minimum data before disclosure;
- use written processor or data-sharing terms where required;
- complete proportionate supplier due diligence and maintain ownership;
- apply current UK adequacy, safeguards and transfer-risk requirements to restricted international transfers; and
- record material disclosures, agreements and decisions.

4.24 Retention, deletion and records

Personal data will be retained only for as long as necessary for the purpose for which it was collected, to meet legal and regulatory obligations, support safeguarding requirements, establish or defend legal claims, and meet legitimate evidential or operational needs.

SDEG maintains a Group Data Retention Schedule as part of its data-protection governance framework. The Schedule sets detailed periods for categories including pupil, safeguarding, SEND, admissions, recruitment, employment, payroll, pension, governance, financial, health and safety, CCTV, complaints, visitor, contractor, marketing and communications records. The

Schedule is maintained by the Chief Operating Officer and is available to staff and on request where appropriate.

Staff must apply the Schedule to records in any format, including email, messaging, paper, images, audio, video and information held within business systems. Records must be filed in an appropriate system so that the applicable retention period can be managed. Email accounts and messaging platforms must not be treated as permanent case-management or record-storage systems.

Information must not be retained indefinitely without a documented legal, safeguarding, operational or archival justification. When the retention period expires and no lawful reason for continued retention exists, information must be securely deleted, destroyed or anonymised. Significant destruction should be authorised and evidenced where appropriate.

Information relating to litigation, legal proceedings, safeguarding matters, complaints, grievances, investigations, rights requests, regulatory action or a formal legal hold must not be destroyed until the matter has concluded and any further retention requirement has been assessed.

Records selected for long-term historical or archival preservation must be identified, justified, secured and managed with appropriate access controls. Proposals to transfer records to a new format or storage environment must consider accessibility, integrity, migration, security and whether a DPIA is required.

4.25 Clear desk and physical records

- secure confidential papers, portable media and devices when unattended;
- lock rooms, cabinets and drawers where appropriate and keep keys secure;
- use confidential waste arrangements and record significant destruction;
- retrieve sensitive printing immediately and avoid unauthorised display;
- do not leave records in vehicles, public places or unsecured household areas; and
- take paper records off site only where necessary and authorised, using secure transport and storage.

4.26 Approved channels, messaging and WhatsApp

- use Group email, Teams and approved systems as the normal channels for Group business;
- do not use WhatsApp to communicate with pupils or parents/carers;
- use WhatsApp for work only where no approved channel is practical, participation is optional and no sensitive, confidential or personal data or photographs are shared;
- keep messages professional and recognise that work-related messages may be disclosable;
- confirm material decisions or arrangements promptly in an official record; and
- leave work groups and remove work content when the working relationship ends, subject to record-retention requirements.

4.27 Remote and flexible working

- apply the same privacy and security standards away from Group premises;
- use approved equipment, accounts, multifactor authentication and secure connectivity;
- prevent household members and other unauthorised people from viewing or using Group information or devices;
- avoid unsecured wireless networks and public conversations or screens;
- store Group work in approved Group locations, not local or unencrypted media;
- secure and dispose of paper records appropriately;
- do not work outside the UK without prior written approval; and
- report loss, theft, compromise, misdirected information or technical problems immediately.

4.28 Automated processing and AI

SDEG will not subject people to solely automated decisions with legal or similarly significant effect unless lawful conditions and safeguards are satisfied. Appropriate transparency, human intervention, the opportunity to express a view and challenge, and a DPIA will be provided where required. AI use is also governed by the AI & Emerging Technologies Policy.

4.29 Incidents and breaches

Every actual or suspected personal data breach must be reported immediately under the Data Incident & Breach Response Protocol. All breaches are documented, whether or not reportable to the ICO. Notifiable breaches are reported without undue delay and, where feasible, within 72 hours of awareness; high-risk breaches are communicated to affected people without undue delay.

5. Monitoring

Staff receive data-protection and cyber-security training at induction and regular refreshers.

The COO will maintain an annual assurance view covering records of processing, privacy notices, rights requests, complaints, breaches, DPIAs, suppliers, training, retention and audit findings.

The Group Board receives annual assurance and material matters are escalated promptly.

At every substantive review by the COO, the policy will be approved by the Group Board.

6. Links with other policies

- Photography, Filming & Image Use Policy;
- Data Incident & Breach Response Protocol;
- SDEG Statutory Privacy Notices;
- Data Retention Schedule;
- Digital Services, Information Security & Cyber Resilience Policy;

- Digital Communications & Acceptable Use Policy;
- AI & Emerging Technologies Policy;
- Safeguarding policies; and
- Risk, Assurance & Compliance Policy.

Appendix A: Key retention principles

The detailed Group Data Retention Schedule is the authoritative operational source for specific retention periods. The principles below summarise the approach that must be applied. This appendix does not replace the detailed Schedule.

Record category	Retention principle
Pupil and admissions records	Retain in accordance with education, safeguarding, limitation and transfer requirements.
Safeguarding and child-protection records	Retain in accordance with statutory safeguarding guidance, inquiry requirements and the Group Data Retention Schedule.
SEND and health records	Retain according to education, health, safeguarding and limitation requirements, with enhanced confidentiality and access controls.
Recruitment records	Retain unsuccessful-candidate information only for the scheduled period unless a lawful and transparent basis supports longer retention. Transfer relevant successful-candidate information to the staff record.
Staff, payroll and pension records	Retain in accordance with employment, tax, pension, insurance, safeguarding and limitation requirements.
Governance, contracts and financial records	Retain to meet statutory, contractual, charity, company, audit, tax and evidential requirements.
CCTV, access and visitor records	Retain for the scheduled operational period unless required for an incident, investigation, safeguarding matter or legal claim.
Complaints, claims and investigations	Retain for the scheduled period and suspend routine destruction while a live matter or legal hold applies.
Marketing, fundraising and consent records	Retain only as necessary for the stated purpose, including evidence of consent, preferences and suppression records required to respect objections.
Emails and messages	Apply the retention period for the subject matter. Move records of lasting value to the appropriate official system or file.
Archival records	Preserve only where there is a documented historical, evidential or public-interest justification and appropriate controls are applied.
Secure disposal	Delete, destroy or anonymise securely when retention expires, subject to any legal hold or continuing lawful need.

Record category	Retention principle
Pupil and admissions records	Retain in accordance with education, safeguarding, limitation and transfer requirements.
Safeguarding and child-protection records	Retain in accordance with statutory safeguarding guidance, inquiry requirements and the Group Data Retention Schedule.
SEND and health records	Retain according to education, health, safeguarding and limitation requirements, with enhanced confidentiality and access controls.
Recruitment records	Retain unsuccessful-candidate information only for the scheduled period unless a lawful and transparent basis supports longer retention. Transfer relevant successful-candidate information to the staff record.
Staff, payroll and pension records	Retain in accordance with employment, tax, pension, insurance, safeguarding and limitation requirements.
Governance, contracts and financial records	Retain to meet statutory, contractual, charity, company, audit, tax and evidential requirements.
CCTV, access and visitor records	Retain for the scheduled operational period unless required for an incident, investigation, safeguarding matter or legal claim.
Complaints, claims and investigations	Retain for the scheduled period and suspend routine destruction while a live matter or legal hold applies.
Marketing, fundraising and consent records	Retain only as necessary for the stated purpose, including evidence of consent, preferences and suppression records required to respect objections.
Emails and messages	Apply the retention period for the subject matter. Move records of lasting value to the appropriate official system or file.
Archival records	Preserve only where there is a documented historical, evidential or public-interest justification and appropriate controls are applied.
Secure disposal	Delete, destroy or anonymise securely when retention expires, subject to any legal hold or continuing lawful need.