



# PRIVACY NOTICES

|                            |                                   |
|----------------------------|-----------------------------------|
| <b>Policy Owner:</b>       | Chief Operating Officer (COO)     |
| <b>ISSR Reference:</b>     | Part 6 – Provision of Information |
| <b>Date of review:</b>     | Summer 2026                       |
| <b>Approved by:</b>        | Group Board                       |
| <b>Date of next review</b> | Autumn 2026                       |

## 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 | Consolidation of statutory privacy notices |

## **1. About these privacy notices**

These are statutory transparency notices, not separate policies. Each notice explains how SDEG processes personal information for a distinct group. The notices should be read with the Data Protection & Privacy Policy and are freely available.

### **1.1 How to use this document**

Go directly to the notice that applies to you. More than one notice may apply, for example where a parent is also a governor, employee or visitor. Additional just-in-time information may be provided for a specific activity. If processing changes materially, the relevant notice will be updated.

### **1.2 How we collect personal information**

SDEG collects personal information in different ways depending on an individual's relationship with the Group.

Most personal information is provided directly by individuals, parents, carers, staff, volunteers, governors, applicants, contractors and visitors through applications, contracts, correspondence, meetings, online systems and day-to-day interactions.

We may also obtain personal information from third parties where appropriate, including:

- previous schools and educational settings;
- referees and former employers;
- the Department for Education, local authorities and safeguarding agencies;
- the Disclosure and Barring Service and the Home Office;
- medical professionals and occupational health providers;
- examination and awarding bodies;
- pension, payroll and recruitment providers;
- professional advisers and approved service providers;
- visitor management, access-control, CCTV and IT systems; and
- publicly available sources where lawful and appropriate.

Where personal information has not been obtained directly from the individual, SDEG will provide privacy information in accordance with UK GDPR requirements. We will make clear whether information is mandatory or optional and, where relevant, the possible consequences of not providing it.

## **2. Notice 1: Pupils, Parents and Carers**

SDEG is the controller for personal information about prospective, current and former pupils and relevant family members and carers.

### **2.1 What we collect**

- identity, contact, family and emergency information;
- admissions, attendance, attainment, assessment and behaviour information;
- SEND, medical, pastoral, safeguarding and welfare information;
- images, recordings, CCTV, access and use of digital systems;
- financial, fee, bursary and payment information;
- co-curricular, trip, transport and catering information;
- characteristics and demographic information; and
- alumni, fundraising and community relationship information.

### **2.2 Why we use it**

- admissions, enrolment and identity;
- education, assessment, reporting and co-curricular provision;
- safeguarding, pastoral, medical, SEND and welfare support;
- attendance, behaviour, security and school operations;
- fees, bursaries, insurance and contractual administration;
- communications, images, community, alumni and fundraising;
- statutory returns, inspection, research, statistics and legal claims; and
- IT security, filtering, monitoring and service improvement.

### **2.3 Lawful bases and sensitive information**

Depending on the purpose, SDEG may rely on one or more of the following lawful bases.

- Consent means that an individual has given clear permission for a specific purpose.
- Contract means that processing is necessary to fulfil a contract or to take steps before entering into one.
- Legal obligation means that processing is necessary to comply with the law.
- Vital interests means that processing is necessary to protect someone's life.
- Public task means that processing is necessary to perform a task in the public interest or an official function that has a clear basis in law.
- Legitimate interests means that processing is necessary for a legitimate organisational purpose, provided that the individual's interests, rights and freedoms do not override those interests.

For this notice, special category information may include health, medical, SEND, safeguarding, racial or ethnic origin, religious or philosophical belief and biometric information where used.

Criminal-offence information may also be processed where lawful. SDEG processes this information only where both a lawful basis and an additional condition apply, including

education or safeguarding obligations, substantial public interest, health or social-care purposes, vital interests, legal claims or explicit consent where appropriate.

Appropriate safeguards are applied. Where consent is relied upon, it may be withdrawn as explained in Annex 1.

## **2.4 Who we may share it with**

- Department for Education, local authorities, ISI and other regulators;
- other schools, examination bodies and education providers;
- health, welfare, safeguarding and law-enforcement bodies;
- professional advisers, insurers and approved service providers;
- catering, transport, clubs, trips and other authorised providers;
- Group schools and authorised staff; and
- fundraising research partners where lawfully used and with applicable opt-out rights.

## **2.5 Retention and security**

Pupil and family records are retained in accordance with safeguarding and education requirements, legal limitation periods, archival value and the specific periods in the SDEG Data Retention Schedule. Copies of the schedule are available on request from the Chief Operating Officer. When information is no longer required, it is securely deleted, destroyed or anonymised as appropriate. SDEG uses appropriate technical and organisational measures designed to protect personal information against accidental loss, unauthorised access, misuse, disclosure, alteration or destruction. These include role-based access controls, approved and secure IT systems, authentication controls, secure transfer methods and encryption where appropriate, supplier due diligence and contractual safeguards, staff training, monitoring and audit controls, secure disposal arrangements and procedures for responding to suspected data-security incidents. Access is limited to people who need the information to perform their duties.

## **2.6 National Pupil Database and statutory collections**

Where legally required, SDEG provides pupil information to the Department for Education. The DfE may retain information in the National Pupil Database and use or share it under its statutory framework. Current DfE privacy information should be consulted for details.

## **2.7 Your rights**

- access personal information and supplementary information;
- ask for inaccurate data to be corrected;
- ask for erasure or restriction where the legal conditions apply;
- object to certain processing, including direct marketing;
- withdraw consent where consent is relied upon;
- request portability where applicable;
- challenge solely automated significant decisions; and
- complain to SDEG and to the ICO.

## **2.8 Contact**

Contact the Chief Operating Officer to ask a question, exercise a right or make a data-protection complaint. Identity and authority may be verified before information is released. You may also contact the ICO.

### **3. Notice 2: Staff**

This notice applies to current and former employees, workers, agency staff and contractors where SDEG processes employment-related information.

#### **3.1 What we collect**

- identity, contact, emergency and family information;
- recruitment, right-to-work, qualifications, references and vetting;
- contract, role, salary, payroll, tax, pension and benefits;
- attendance, leave, health, occupational health and adjustments;
- performance, development, grievance, conduct and disciplinary records;
- equality monitoring and trade-union information;
- criminal-record information where lawful;
- CCTV, access, IT use, communications and security monitoring; and
- termination and post-employment information.

#### **3.2 Why we use it**

- recruitment, appointment and employment administration;
- pay, pension, benefits and workforce planning;
- training, performance, progression and professional development;
- sickness, welfare, adjustments, health and safety;
- safeguarding, vetting, security and fraud prevention;
- employee relations, complaints, investigations and legal claims;
- equality monitoring and statutory reporting; and
- continuity, insurance, audit and regulatory compliance.

#### **3.3 Lawful bases and sensitive information**

Depending on the purpose, SDEG may rely on one or more of the following lawful bases.

- Consent means that an individual has given clear permission for a specific purpose.
- Contract means that processing is necessary to fulfil a contract or to take steps before entering into one.
- Legal obligation means that processing is necessary to comply with the law.
- Vital interests means that processing is necessary to protect someone's life.
- Public task means that processing is necessary to perform a task in the public interest or an official function that has a clear basis in law.
- Legitimate interests means that processing is necessary for a legitimate organisational purpose, provided that the individual's interests, rights and freedoms do not override those interests.

For this notice, special category information may include health, medical, SEND, safeguarding, racial or ethnic origin, religious or philosophical belief and biometric information where used.

Criminal-offence information may also be processed where lawful. SDEG processes this information only where both a lawful basis and an additional condition apply, including education or safeguarding obligations, substantial public interest, health or social-care purposes, vital interests, legal claims or explicit consent where appropriate.

Appropriate safeguards are applied. Where consent is relied upon, it may be withdrawn as explained in Annex 1.

### **3.4 Who we may share it with**

- HMRC, pension and benefits providers;
- DfE, DBS, teaching and regulatory bodies;
- occupational health, insurers, advisers and payroll providers;
- law enforcement, local authorities and safeguarding agencies;
- approved IT, HR and other processors;
- prospective employers where a lawful reference is provided; and
- other Group schools and authorised managers.

### **3.5 Retention and security**

Employment records are retained in accordance with legal obligations, safeguarding requirements, pension and insurance needs, disputes, limitation periods and the specific periods in the SDEG Data Retention Schedule. Copies of the schedule are available on request from the Chief Operating Officer. When information is no longer required, it is securely deleted, destroyed or anonymised as appropriate. SDEG uses appropriate technical and organisational measures designed to protect personal information against accidental loss, unauthorised access, misuse, disclosure, alteration or destruction. These include role-based access controls, approved and secure IT systems, authentication controls, secure transfer methods and encryption where appropriate, supplier due diligence and contractual safeguards, staff training, monitoring and audit controls, secure disposal arrangements and procedures for responding to suspected data-security incidents. Access is limited to people who need the information to perform their duties.

### **3.6 Your rights**

- access personal information and supplementary information;
- ask for inaccurate data to be corrected;
- ask for erasure or restriction where the legal conditions apply;
- object to certain processing, including direct marketing;
- withdraw consent where consent is relied upon;
- request portability where applicable;
- challenge solely automated significant decisions; and
- complain to SDEG and to the ICO.

### **3.7 Contact**

Contact the Chief Operating Officer to ask a question, exercise a right or make a data-protection complaint. Identity and authority may be verified before information is released. You may also contact the ICO.

## **4. Notice 3: Job Applicants**

This notice applies to people applying for employment or engagement with SDEG. Successful applicants will also receive the Staff Privacy Notice.

### **4.1 What we collect**

- identity, contact, employment, education and qualification information;
- application, interview, assessment and correspondence;
- references, right-to-work, professional status and online-search information;
- health, disability and adjustment information;
- equality-monitoring information; and
- criminal-record and safeguarding information where lawful and appropriate.

### **4.2 Why we use it**

- manage applications and communications;
- assess qualifications and suitability;
- make reasonable adjustments;
- carry out safer-recruitment, reference and vetting checks;
- monitor equality and recruitment effectiveness;
- meet legal and regulatory obligations; and
- establish, exercise or defend legal claims.

### **4.3 Lawful bases and sensitive information**

Depending on the purpose, SDEG may rely on one or more of the following lawful bases.

- Consent means that an individual has given clear permission for a specific purpose.
- Contract means that processing is necessary to fulfil a contract or to take steps before entering into one.
- Legal obligation means that processing is necessary to comply with the law.
- Vital interests means that processing is necessary to protect someone's life.
- Public task means that processing is necessary to perform a task in the public interest or an official function that has a clear basis in law.
- Legitimate interests means that processing is necessary for a legitimate organisational purpose, provided that the individual's interests, rights and freedoms do not override those interests.

For this notice, special category information may include health, medical, SEND, safeguarding, racial or ethnic origin, religious or philosophical belief and biometric information where used.

Criminal-offence information may also be processed where lawful. SDEG processes this information only where both a lawful basis and an additional condition apply, including education or safeguarding obligations, substantial public interest, health or social-care purposes, vital interests, legal claims or explicit consent where appropriate.

Appropriate safeguards are applied. Where consent is relied upon, it may be withdrawn as explained in Annex 1.

#### **4.4 Who we may share it with**

- referees and former employers;
- TES, recruitment agencies and assessment providers;
- DBS, Home Office, DfE and professional bodies;
- occupational health and approved advisers;
- authorised Group staff and schools; and
- law enforcement or regulators where required.

#### **4.5 Retention and security**

Unsuccessful application records are retained for the period specified in the SDEG Data Retention Schedule and then securely deleted. Information relating to a successful candidate is transferred to the staff record where appropriate. Copies of the schedule are available on request from the Chief Operating Officer. When information is no longer required, it is securely deleted, destroyed or anonymised as appropriate. SDEG uses appropriate technical and organisational measures designed to protect personal information against accidental loss, unauthorised access, misuse, disclosure, alteration or destruction. These include role-based access controls, approved and secure IT systems, authentication controls, secure transfer methods and encryption where appropriate, supplier due diligence and contractual safeguards, staff training, monitoring and audit controls, secure disposal arrangements and procedures for responding to suspected data-security incidents. Access is limited to people who need the information to perform their duties.

#### **4.6 Your rights**

- access personal information and supplementary information;
- ask for inaccurate data to be corrected;
- ask for erasure or restriction where the legal conditions apply;
- object to certain processing, including direct marketing;
- withdraw consent where consent is relied upon;
- request portability where applicable;
- challenge solely automated significant decisions; and
- complain to SDEG and to the ICO.

#### **4.7 Contact**

Contact the Chief Operating Officer to ask a question, exercise a right or make a data-protection complaint. Identity and authority may be verified before information is released. You may also contact the ICO.

## **5. Notice 4: Governors and Volunteers**

This notice applies to Group Board Members, Local School Board members, volunteers and applicants for those roles.

### **5.1 What we collect**

- identity, contact, emergency and biographical information;
- application, appointment, skills, training and governance records;
- interests, conflicts, expenses and meeting participation;
- references, safeguarding, DBS and suitability information;
- images, website profile and communications;
- equality-monitoring information; and
- CCTV, access and use of Group systems.

### **5.2 Why we use it**

- appointment, suitability and statutory governance records;
- safeguarding, training and role administration;
- meetings, decisions, minutes, panels and assurance;
- conflicts, declarations, expenses and regulatory reporting;
- communications, website information and stakeholder engagement;
- security, investigation, complaints and legal claims; and
- governance review, succession and development.

### **5.3 Lawful bases and sensitive information**

Depending on the purpose, SDEG may rely on one or more of the following lawful bases.

- Consent means that an individual has given clear permission for a specific purpose.
- Contract means that processing is necessary to fulfil a contract or to take steps before entering into one.
- Legal obligation means that processing is necessary to comply with the law.
- Vital interests means that processing is necessary to protect someone's life.
- Public task means that processing is necessary to perform a task in the public interest or an official function that has a clear basis in law.
- Legitimate interests means that processing is necessary for a legitimate organisational purpose, provided that the individual's interests, rights and freedoms do not override those interests.

For this notice, special category information may include health, medical, SEND, safeguarding, racial or ethnic origin, religious or philosophical belief and biometric information where used.

Criminal-offence information may also be processed where lawful. SDEG processes this information only where both a lawful basis and an additional condition apply, including education or safeguarding obligations, substantial public interest, health or social-care purposes, vital interests, legal claims or explicit consent where appropriate.

Appropriate safeguards are applied. Where consent is relied upon, it may be withdrawn as explained in Annex 1.

#### **5.4 Who we may share it with**

- DfE, Companies House, Charity Commission and regulators where applicable;
- DBS, local authorities and safeguarding bodies;
- professional advisers, insurers and approved providers;
- authorised staff and other Group governance bodies; and
- law enforcement or courts where required.

#### **5.5 Retention and security**

Governance and volunteer records are retained in accordance with statutory registers, governance history, safeguarding and limitation requirements and the specific periods in the SDEG Data Retention Schedule. Copies of the schedule are available on request from the Chief Operating Officer. When information is no longer required, it is securely deleted, destroyed or anonymised as appropriate. SDEG uses appropriate technical and organisational measures designed to protect personal information against accidental loss, unauthorised access, misuse, disclosure, alteration or destruction. These include role-based access controls, approved and secure IT systems, authentication controls, secure transfer methods and encryption where appropriate, supplier due diligence and contractual safeguards, staff training, monitoring and audit controls, secure disposal arrangements and procedures for responding to suspected data-security incidents. Access is limited to people who need the information to perform their duties.

#### **5.6 Your rights**

- access personal information and supplementary information;
- ask for inaccurate data to be corrected;
- ask for erasure or restriction where the legal conditions apply;
- object to certain processing, including direct marketing;
- withdraw consent where consent is relied upon;
- request portability where applicable;
- challenge solely automated significant decisions; and
- complain to SDEG and to the ICO.

#### **5.7 Contact**

Contact the Chief Operating Officer to ask a question, exercise a right or make a data-protection complaint. Identity and authority may be verified before information is released. You may also contact the ICO.

## **6. Notice 5: Visitors and Contractors**

This notice applies to visitors, contractors, consultants, supplier personnel and others attending sites or accessing Group systems.

### **6.1 What we collect**

- identity, contact, organisation and visit details;
- arrival, departure, vehicle, access-control and CCTV information;
- safeguarding, DBS, competency and contractor checks where required;
- health, safety, emergency and access-adjustment information;
- contract, service, invoice and communication information; and
- system, network, remote-access and security information.

### **6.2 Why we use it**

- manage safe and orderly access to premises and systems;
- safeguarding, health and safety and emergency response;
- administer services, contracts, payment and supplier relationships;
- protect people, property, networks and information;
- investigate incidents, fraud, complaints and legal claims; and
- meet legal, regulatory, insurance and audit requirements.

### **6.3 Lawful bases and sensitive information**

Depending on the purpose, SDEG may rely on one or more of the following lawful bases.

- Consent means that an individual has given clear permission for a specific purpose.
- Contract means that processing is necessary to fulfil a contract or to take steps before entering into one.
- Legal obligation means that processing is necessary to comply with the law.
- Vital interests means that processing is necessary to protect someone's life.
- Public task means that processing is necessary to perform a task in the public interest or an official function that has a clear basis in law.
- Legitimate interests means that processing is necessary for a legitimate organisational purpose, provided that the individual's interests, rights and freedoms do not override those interests.

For this notice, special category information may include health, medical, SEND, safeguarding, racial or ethnic origin, religious or philosophical belief and biometric information where used.

Criminal-offence information may also be processed where lawful. SDEG processes this information only where both a lawful basis and an additional condition apply, including education or safeguarding obligations, substantial public interest, health or social-care purposes, vital interests, legal claims or explicit consent where appropriate.

Appropriate safeguards are applied. Where consent is relied upon, it may be withdrawn as explained in Appendix 1.

## **6.4 Who we may share it with**

- the visitor or contractor's organisation;
- DBS, safeguarding bodies and regulators;
- law enforcement, emergency services and local authorities;
- professional advisers, insurers and approved service providers; and
- authorised staff and Group schools.

## **6.5 Retention and security**

Visitor and contractor information is retained in accordance with security, safeguarding, contractual, financial and legal requirements and the specific periods in the SDEG Data Retention Schedule. Copies of the schedule are available on request from the Chief Operating Officer. When information is no longer required, it is securely deleted, destroyed or anonymised as appropriate. SDEG uses appropriate technical and organisational measures designed to protect personal information against accidental loss, unauthorised access, misuse, disclosure, alteration or destruction. These include role-based access controls, approved and secure IT systems, authentication controls, secure transfer methods and encryption where appropriate, supplier due diligence and contractual safeguards, staff training, monitoring and audit controls, secure disposal arrangements and procedures for responding to suspected data-security incidents. Access is limited to people who need the information to perform their duties.

## **6.6 Your rights**

- access personal information and supplementary information;
- ask for inaccurate data to be corrected;
- ask for erasure or restriction where the legal conditions apply;
- object to certain processing, including direct marketing;
- withdraw consent where consent is relied upon;
- request portability where applicable;
- challenge solely automated significant decisions; and
- complain to SDEG and to the ICO.

## **6.7 Contact**

Contact the Chief Operating Officer to ask a question, exercise a right or make a data-protection complaint. Identity and authority may be verified before information is released. You may also contact the ICO.

## **Annex 1: Common information for all notices**

### **A1.1 Controller and DPO contact**

St Dunstan's Education Group is the controller for the purposes of UK GDPR and the Data Protection Act 2018. Questions, concerns, rights requests and complaints should initially be directed to the Chief Operating Officer.

SDEG has appointed Judicium Consulting Limited to provide Data Protection Officer services and independent advice regarding compliance with data protection legislation.

Data Protection Officer: Judicium Consulting Limited Address: 5th Floor, 98 Theobalds Road, London WC1X 8WB Email: [dataservices@judicium.com](mailto:dataservices@judicium.com) Website: [www.judiciumeducation.co.uk](http://www.judiciumeducation.co.uk)

Individuals may also complain to the Information Commissioner's Office, the UK supervisory authority for data protection matters.

### **A1.2 Indirect collection**

In addition to information provided directly by individuals, SDEG may receive personal information from:

- parents, carers and family members;
- former schools or employers;
- referees; local authorities and safeguarding agencies;
- government departments;
- professional and regulatory bodies;
- medical and occupational-health professionals;
- examination and awarding bodies;
- recruitment, payroll and pension providers;
- online application and visitor systems;
- approved service providers;
- CCTV, access-control and SDEG IT systems;
- and publicly available sources where lawful and appropriate.

Where UK GDPR requires privacy information to be provided following indirect collection, SDEG will provide it within the applicable period.

### **A1.3 International transfers**

Where personal information is transferred outside the UK, SDEG will use an applicable adequacy decision, recognised safeguard or other lawful mechanism and will assess risks where required.

### **A1.4 Automated decision-making**

SDEG does not ordinarily make solely automated decisions with legal or similarly significant effect. If such processing is proposed, SDEG will provide the required information and safeguards, including human intervention and a route to challenge.

### **A1.5 Withdrawing consent**

Where SDEG relies on consent, the individual may withdraw that consent at any time by contacting the Chief Operating Officer. Withdrawal will not affect the lawfulness of processing carried out before consent was withdrawn. Once consent is withdrawn, SDEG will stop the processing covered by that consent unless another lawful basis applies. Where possible, withdrawing consent will be as easy as giving it.

### **A1.6 Data protection complaints**

A complaint may be made verbally or in writing through any reasonable channel. SDEG will acknowledge it within 30 days, take appropriate steps to investigate without undue delay, keep the complainant informed and communicate the outcome without undue delay. This does not remove the right to complain to the ICO.