ST ALBANS
EDUCATION GROUP

Data Protection

September 2026

A group of sector-leading Independent Schools

PART OF

STAHS Policies

P14: DATA PROTECTION POLICY

Owner/s:	Chief Operating Officer	Date reviewed:	September 2026
Date ratified:	Due to be ratified	Next review date:	September 2027
STAEG Committee:	STAEG Council		

Contents

1. BACKGROUND....3
2. DEFINITIONS....3
3. APPLICATION OF THIS POLICY....4
4. PERSON RESPONSIBLE FOR DATA PROTECTION AT THE SCHOOL....4
5. THE PRINCIPLES....4
6. LAWFUL GROUNDS FOR DATA PROCESSING....5
7. HEADLINE RESPONSIBILITIES OF ALL STAFF....5
8. RIGHTS OF INDIVIDUALS....7
9. DATA SECURITY: ONLINE AND DIGITAL....7
10. PROCESSING OF FINANCIAL / CREDIT CARD DATA....8
11. SUMMARY....8

1. BACKGROUND

1.1. Data protection is an important legal compliance issue for the School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notices). The School, as 'data controller', is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring the School complies with, and is mindful of, its legal obligations, whether that personal data handling is sensitive or routine.

1.2. UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018) as supplemented and amended by the Data (Use and Access) Act 2025. The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of safeguarding obligations, and regarding the right of access to personal data.

1.3. Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. DEFINITIONS

Key data protection terms used in this Data Protection Policy are:

Data controller	a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller
Data processor	an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
Data handler	a person or body that collects, processes, stores, uses, shares or disposes of data as part of their role
Personal data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Personal information (or 'personal data')	any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
Processing	virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
Special categories of personal data	data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual

	orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. APPLICATION OF THIS POLICY

3.1. This Policy sets out the School's expectations and procedures with respect to processing any personal data the School collects from data subjects (including parents, pupils, employees, contractors and third parties).

3.2. Those who handle personal data as employees or governors of the School are obliged to comply with this Policy when doing so. For employees, breaches of this Policy may result in disciplinary action. Accidental breaches of the law or this Policy in handling personal data will happen from time to time, for example by human error, and will not always be treated a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

3.3. In addition, this Policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

3.4. Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this Policy.

3.5. Volunteers and contractors will be data controllers in their own right, but the same legal regime and best practice standards set out in this Policy will apply by law.

4. PERSON RESPONSIBLE FOR DATA PROTECTION AT THE SCHOOL

4.1. The Chief Operating Officer is the Data Protection Lead for the Group who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. The Director of IT acts as the Deputy Data Protection Lead for the Group. Each school is to nominate a member of its SLT as a School Data Protection Lead. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Lead.

5. THE PRINCIPLES

5.1. The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

5.1.1. Processed lawfully, fairly and in a transparent manner;

5.1.2. Collected for specific and explicit purposes and only for the purposes it was collected for;

5.1.3. Relevant and limited to what is necessary for the purposes it is processed;

5.1.4. Accurate and kept up to date;

5.1.5. Kept for no longer than is necessary for the purposes for which it is processed; and

5.1.6. Processed in a manner that ensures appropriate security of the personal data.

5.2. The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that it is also able to demonstrate that its processing is lawful. This involves, among other things:

5.2.1. Keeping records of its data processing activities, including by way of logs and policies;

5.2.2. Documenting significant decisions and assessments about how it uses personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and

5.2.3. Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how Privacy Notice(s) are updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. LAWFUL GROUNDS FOR DATA PROCESSING

6.1. Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

6.2. One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notices, as GDPR requires.

6.3. Other lawful grounds include:

6.3.1. Compliance with a legal obligation, including in connection with employment, engagement of services and diversity;

6.3.2. Contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;

6.3.3. A narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. HEADLINE RESPONSIBILITIES OF ALL STAFF

7.1. Record-keeping

7.1.1. It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if they are dissatisfied with how it has been recorded. This applies to how staff record their own data, and personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

7.1.2. Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

7.2. Data handling

7.2.1. All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all the relevant School policies and procedures to the extent applicable to them. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, and so all staff should in read and comply with the relevant policies listed below within these areas.

- 01 Safeguarding & Child Protection (and related documents)

- 10 Admissions (and related documents)
- 11 Complaints (and related documents)
- 15 Internet Enabled Devices (and related documents)
- 16 HR and Employment (and related documents)
- 17 Finance Policy (and related documents)

7.2.2. Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

7.3. Avoiding, mitigating and reporting data breaches

7.3.1. One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

7.3.2. In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether the School needs to notify the ICO. If staff become aware of a personal data breach, they must notify the Data Protection Lead, and in their absence, the Group Data Protection Lead. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not, but the School always needs to know about them to make a decision.

7.3.3. As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the applicable staff member's contract.

7.4. Card and data security

7.4.1. More generally, the School requires all staff (and expects all its contractors) to remain mindful of the data protection principles (see section 5 above) and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers (see Section 2) should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

7.4.2. The School expects all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the School Data Protection Lead, and to identity the need for (and implement) regular staff training. Staff must attend any training required by the School.

7.5. Use of third part platforms/suppliers.

7.5.1. As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high-risk form of processing (including most uses of artificial intelligence (AI) technology). Any request to engage a third-party supplier should be referred to the School Data Protection Lead in the first instance, and at as early stage as possible. Further advice may be sought form the Group Data Protection Lead (or deputy) as required.

8. RIGHTS OF INDIVIDUALS

8.1. In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller

(i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If any individual becomes aware of a subject access request (or indeed any communication from an individual about their personal data), they must tell the School Data Protection Lead, as soon as possible. The Group Data Protection Lead will provide advice and guidance as required.

8.2. Individuals also have legal rights to:

8.2.1. Require the School to correct the personal data held about them if it is inaccurate;

8.2.2. Request that the School erases their personal data (in certain circumstances);

8.2.3. Request that the School restricts its data processing activities (in certain circumstances);

8.2.4. Receive from the School the personal data it holds about them for the purpose of transmitting it in a commonly used format to another data controller; and

8.2.5. Object, on grounds relating to their particular situation, to any of the School's particular processing activities where the individual feels this has a disproportionate impact on them.

8.2.6. Complain to the School about a data protection issue.

8.3. None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

8.3.1. Contest or seek human intervention in cases of solely automated individual decision-making (i.e. where a significant decision is made about the individual without human intervention);

8.3.2. Object to direct marketing; and

8.3.3. Withdraw one's consent where the School is relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

8.4. In any event, however, if a request from an individual who is purporting to exercise one or more of their data protection rights is received, the School Data Protection Lead must be informed as soon as possible.

9. DATA SECURITY: ONLINE AND DIGITAL

9.1. The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data:

9.1.1. No member of staff is permitted to remove unsecured personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the School Data Protection Lead.

9.1.2. Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.

9.1.3. Use of personal email accounts or unencrypted personal devices by staff for official School business is not permitted.

9.1.4. No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so and where required, a data protection impact assessment has been completed to the satisfaction of the School Data Protection Lead and/or the Group Data Protection Lead, as appropriate.

10. PROCESSING OF FINANCIAL / CREDIT CARD DATA

10.1. The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. Staff who are unsure in this regard should please seek further guidance from the Group Director of Finance.

10.2. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details), may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. SUMMARY

11.1. It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly. A good rule of thumb is to ask questions such as:

11.1.1. Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?

11.1.2. Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?

11.1.3. What would be the consequences of my losing or misdirecting this personal data?

11.2. Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how to handle and record personal information and manage the School's relationships with people. This is an important part of the School's culture, and all its staff and representatives need to be mindful of it.