SEVENOAKS SCHOOL

Policy reference	BD1
Policy Category	Operations, resources and compliance-related policies
Name of policy	Data Protection Policy
Purpose of policy	Data protection is an important legal compliance issue for Sevenoaks School. The school collects, stores and processes personal data about staff, pupils, their parents, its contractors and other third parties. All staff have a part to play in ensuring we comply with and are mindful of our legal obligations.
Scope	Sevenoaks School (senior) Staff, students, parents
Regulatory or legal requirement addressed by policy	UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), and the Data (Use and Access) Act 2025 ("DUAA"),
Other policies referred to	IT Terms of Use Online Safety Policy Privacy statement (School)
Policy owned by	Data Protection Officer
Date effective from	V1.0 August 2019 V2.0 – 27 June 2024 V3.0- 25 February 2025 V3.1 1 November 2025 V4 March 2026
Published on website/external facing	Yes

1. Background

Data protection is an important legal compliance issue for Sevenoaks School (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 Statement). The school, as data "controller", is liable for the actions of its staff in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

The School processes personal data in accordance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), and the Data (Use and Access) Act 2025 ("DUAA"), together with any related legislation and guidance issued by the Information Commissioner. The Information Commissioner regulates data protection law in the UK and issues guidance on the interpretation and application of data protection legislation.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 in the UK 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 is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.

- **Data Processor** – an organisation that processes personal data on behalf of a 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.

- **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 data, 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

This policy sets out the school's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees 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 as a disciplinary issue. However, failure to report breaches that pose significant risks to the school or individuals will be considered a serious matter.

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 'processors' on the school's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party controllers – which may range from other schools to parents and appropriate authorities – 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.

Under certain circumstances and where appropriate and lawful to do so, the school will share personal data with Sevenoaks School Foundation and vice versa for their respective purposes. Where personal data is shared, it is always in compliance with data protection laws.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

4. Person responsible for Data Protection at the School

The school has appointed a Data Protection Officer who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. 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 Officer (DPO@sevenoaksschool.org).

5. The Principles

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

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;

4. **Accurate** and kept **up to date**;

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

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

The UK GDPR's broader 'accountability' principle also requires that the school not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were 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

Under the UK 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 the UK 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.

The School may also rely on "recognised legitimate interests" where permitted by law. These are specific processing activities identified in legislation as being in the public interest and which do not require a balancing test between organisational interests and the rights of individuals. Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- 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

Record-keeping

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 you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal

data of others, in particular colleagues, pupils and their parents, in a way that is professional and appropriate.

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 that information. This absolutely must not discourage staff from making 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 write 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.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and all 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, so all staff should read and comply with the following policies:

- Safeguarding Policy; Online Safety Policy, IT Terms Use Terms; Behaviour Policy; policies relating to the use of photographs.

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.

Avoiding, mitigating and reporting data breaches

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

In addition, 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 we need to notify the ICO. If staff become aware of a personal data breach, they must notify the Data Protection Officer. 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.

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.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 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 effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Data Protection Officer, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third-party platforms / suppliers

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 be necessary to complete a Data Protection Impact Assessment (DPIA) before proceeding, including carrying out a due diligence exercise – particularly if the platform or software involves any sort of novel or high-risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third-party supplier should be referred to the Data Protection Officer in the first instance, and at as early a stage as possible.

Use of AI Tools for Meeting Recording and Transcription

The School permits the use of School-approved AI tools (such as Microsoft Copilot) on school-managed devices for the purpose of recording and transcribing meetings, provided that:

- Informed consent is obtained from all participants before recording begins;
- Recordings and AI-generated transcripts are processed, stored, and retained securely in accordance with this policy;
- Access to recordings and transcripts is restricted to authorised personnel only;
- Recordings are retained only for as long as necessary to fulfil their purpose, after which they must be securely deleted.
- Personal data must not be entered into unapproved AI tools or generative AI systems.
- Any use of AI technology involving personal data must be assessed for data protection risks and may require a Data Protection Impact Assessment (DPIA).
- Staff must ensure that AI-generated outputs are reviewed for accuracy and appropriateness before use.

8. Rights of Individuals

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 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. When responding to a subject access request, the School will carry out reasonable and proportionate searches for personal data in accordance with applicable legislation and guidance. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Data Protection Officer as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;

- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

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:

- be informed about significant decisions made about them through automated processing; request human intervention in relation to such decisions; make representations about the decision; and challenge or contest the outcome of automated decision-making. Object to direct marketing; and
- withdraw one's consent where we are 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).

Complaints

Individuals have the right to raise a complaint with the School if they believe their personal data has been processed in a way that does not comply with data protection law.

The School will provide a clear process for individuals to submit complaints relating to the processing of their personal data. Complaints will be acknowledged within 30 days and responded to without undue delay. Individuals also retain the right to complain to the Information Commissioner.

In any event, however, if you receive a request from an individual who is intending to exercise one or more of their data protection rights, you must tell the Data Protection Officer as soon as possible (DPO@sevenoaksschool.org).

9. Data Security: online and digital

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. All staff are required read the Online Safety Policy and sign the IT Terms of Use, prior to accessing the school IT. Breaching the Policy or IT Terms of Use may result in withdrawal of school network access and disciplinary action up to and including dismissal.

10. Data Retention

The School will retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including to meet legal, regulatory, safeguarding and operational requirements.

The School maintains a separate Data Retention Schedule which sets out the retention periods for different categories of personal data. Staff must ensure that personal data is managed in accordance with this schedule.

When personal data is no longer required it will be securely deleted, destroyed or anonymised in accordance with the School's data security procedures.

Staff should consult the Data Protection Officer if they are unsure about the appropriate retention period for any category of personal data.

11. International data transfer

Personal data may be transferred outside the United Kingdom where appropriate safeguards are in place. These safeguards may include adequacy regulations issued by the UK government, standard contractual clauses, or other legally recognised transfer mechanisms.

Any international data transfers must be approved by the Data Protection Officer prior to the transfer taking place.

12. Processing of Financial / Credit Card Data

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. If you are unsure in this regard, please seek further guidance from the Director of Finance. 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.

13. Privacy Statements

Further information on how the School processes personal data can be found on the schools Privacy Statement | Sevenoaks School, additional information how the Sevenoaks School Foundation processes personal data can be found at Privacy Statement | The Foundation.