

Data Protection Policy

Applies to:

- All staff (teaching and non-teaching), the directors and volunteers working in the School.
- Pupils, Parents, Guardians and Caregivers and Prospective Pupils
- Visitors and Contractors

Availability:

This policy is made available in the following ways:

- The School's website www.radnor-sevenoaks.org;
- Via Teams, All Staff Shared Documents, Compliance, Policies;
- On request a copy may be obtained from the School's Office.

Monitoring and Review:

- This policy will be subject to continuous monitoring, refinement and audit by the Head.
- The Board of Directors undertake a formal annual review of this policy.

Signed:



David Paton
Head



Ian Davies
Chairman of the Board of Directors

Reviewed on: September 2025

Next Review: September 2026

1. Background

- 1.1. Data protection is an important legal compliance issue for Radnor House Sevenoaks (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 Notice. The School, as data "controller", is liable for the actions of its staff, directors and governors 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.
- 1.2. UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018"). The DPA 2018 includes specific provisions relevant to independent schools, particularly in the context of our 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 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

- 2.1. 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 its directors and governors) 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

- 3.1. 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).
- 3.2. 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.
- 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 '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.
- 3.4. 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.

4. Person responsible for Data Protection at the School

- 4.1. The School has appointed Rachel Nemchand as the Data Protection Co-ordinator 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 Co-ordinator.

5. The Principles

- 5.1. The UK GDPR outlines six principles governing the processing of personal data that controllers (and processors) must adhere to. These require that personal data must be:
 - Processed lawfully, fairly and in a transparent manner;
 - Collected for specific and explicit purposes and only for the purposes it was collected for;
 - Relevant and limited to what is necessary for the purposes it is processed;
 - Accurate and kept up to date;
 - Kept for no longer than is necessary for the purposes for which it is processed; and
 - Processed in a manner that ensures appropriate security of the personal data.

5.2. 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

6.1. 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.

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 School 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 Notice, as the UK GDPR requires.

6.3. 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

7.1. 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 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

- 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 online safety.
- 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

- 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 Compliance Officer Rachel Nemchand. 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.

7.4. 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 particular champions of these principles and to oversee the swift reporting of any concerns about how the School uses personal information, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

8. Use of third-party platforms/suppliers

8.1. 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 any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to Mark Leporati in the first instance, and at as early a stage as possible.

9. Rights of Individuals

9.1. 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 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 you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the compliance officer as soon as possible.

9.2. 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.

9.3. 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:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- 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).

9.4. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Head or the Compliance Officer as soon as possible.

10. Data Security: online and digital

10.1. 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.

- No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head.
- 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.]
- Memory sticks or personal devices are not permitted in the School.
- Use of personal email accounts or [unencrypted] personal devices by or staff for official School business is not permitted.

11. Processing of Financial / Credit Card Data

11.1. 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. If you are unsure in this regard please seek further guidance from the Director of Finance and Operations. 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 a material impact on individuals and should be handled accordingly.

Appendix A - The Recording of Telephone Calls To / From the School

1. Introduction

Radnor House Sevenoaks has an automatic telephone recording system which records calls made to, and from, the School using the external VOIP telephone system.

Purpose of Call Recording

- The School records telephone calls to ensure:
 - operational efficiency, the ability to check on facts discussed during a call;
 - safeguarding or pastoral concerns can be properly addressed;
 - enhanced communication; and
 - staff training.
 - The system will be provided and operated in a way that is consistent with an individual's right to privacy.
- The system will **NOT** be used to:
 - provide data to the World Wide Web.
 - disclose to the media.

2. Owner

- The telephone recording system is owned by Radnor House Sevenoaks School.
- The Director of Finance and Operations is responsible for the day-to-day operation of the system and ensuring compliance with this policy.
- Contact details: The Director of Finance and Operations, Radnor House Sevenoaks School, 01959-563720

3. Overview of System

- The VOIP system runs on 44 telephone handsets in the School, recording both incoming and outgoing telephone calls.
- Callers dialling into the School will hear an automated message informing them of this fact, and there is further information on the School website, and in this policy.
- The School is able to access and listen again to the content of these calls using the telephone management system. The system does not record internal telephone calls.
- If a caller does not wish to continue with a recorded call, they are encouraged to contact the School in person, by email or by letter.
- The telephone recording system runs twenty-four hours a day, seven days a week.
- Recordings are deleted automatically by the system after 12 weeks.
- The telephone recording system is managed by School staff and the School's VOIP provider acting on the School's behalf.
- The recordings are held securely by the School's VOIP provider, who is fully GDPR-compliant.
- There is no routine monitoring of calls. The recordings will only be accessed in response to a specific query.
- Details of access to calls will be logged, together with the reasons for access, which will principally be for operational efficiency, security/safety purposes or staff training.
- A monitoring system is in place to ensure the system is used securely, and that confidentiality is maintained.

4. Access to Recordings

- Access to the recordings will be restricted to the Head, the Head of IT and two other members of the senior leadership team.
- Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following:
 - Police and other law enforcement agencies where the content recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
 - Prosecution agencies.
 - People whose calls have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).

5. Individual Access Rights

- The Act gives individuals the right to access personal information about themselves, including telephone call recordings.
- All requests for access to a copy of call recordings by individuals should be made in writing to the School's Director of Finance and Operations, using a Subject Access Request form available from the School office. The Director of Finance and Operations will liaise with relevant staff to determine whether disclosure of the content will reveal third party information.
- Requests for access to call recordings must include:
 - The date and time the call was recorded
 - Information to identify the individuals involved in the call, if necessary
 - Proof of Identity
- The School will respond promptly, at the latest within one month of receiving the request, if sufficient information is provided to identify the call requested.
- If the School cannot comply with the request, the reasons will be documented.
- The requester will be advised of these in writing, where possible.

6. Access to Call Recordings by Third Parties

- Unlike Data Subjects, third parties who wish to have a copy of call recordings (i.e not the person involved in the call) do not have a right of access to data under the DPA, and care must be taken when complying with such requests to ensure that neither the DPA, HRA or this Policy are breached. As noted above, requests from third parties will only be granted if the requestor falls within the following categories:
 - Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
 - Prosecution agencies
 - Appropriate members of School staff (such as Human Resources) to ensure compliance with the School's regulations and policies.
- All third party requests for access to a call recording by third parties should be made in writing to the

School's Director of Finance and Operations, who will liaise with relevant security staff to determine whether disclosure of the call will reveal third-party information.

7. Retention and Disposal

- Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded calls will be retained for no longer than 12 weeks from the date of recording.
- At the end of their useful life, all call recordings will be automatically erased and securely disposed of as confidential waste.

8. Complaints

Complaints regarding the call recording system and its operation must be made in writing to the Director of Finance and Operations.