The Sheiling
Ringwood
A learning and caring community
where individuals are valued

1J DATA PROTECTION POLICY

Reviewed: KK / May 2023 (Annually)
Ratified by Board of Trustees: June 2023
Next Review date: Summer Term 2024
EDI Assessment: SSET does not currently identify any EDI impact of this policy; should new information come to light, this will be considered at the next review.

1 Aims

The Sheiling Special Education Trust ("SSET"/"we") aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.
- It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

3 Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4 The data controller

SSET processes personal information relating to parents, students, staff, trustees, visitors and others, and is the data controller for the purposes of data protection. SSET is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5 Roles and responsibilities

This policy applies to all staff employed by SSET, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Board of Trustees

The trustee board has overall responsibility for ensuring that SSET complies with all relevant data protection obligations.

Data Protection Lead

The Data Protection Lead (DPL) at SSET is responsible for:

- overseeing the implementation of this policy;
- monitoring our compliance with data protection law;
- advising SSET and its staff on its data protection obligations; and
- developing related policies and guidelines, where applicable. To this end, and where appropriate, the DPL will take professional advice and guidance.

The DPL is the first point of contact for individuals whose data SSET processes, and for the ICO. If you have any questions or comments about the content of this policy or if you need further information, you should contact the DPL.

The DPL is the Head of Finance & Premises and is contactable via The Sheiling Ringwood, Horton Road, Ashley, Ringwood, Hants, BH24 2EB or via email: dataprotection@thesheilingringwood.co.uk

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing SSET of any changes to their personal data, such as a change of address;
- Contacting the DPL in the following circumstances:
  - With any concerns about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - If they have any concerns that this policy is not being followed;

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
- If there has been a data breach;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they need help with any contracts or sharing personal data with third parties.

6 Data protection principles

UK GDPR is based on data protection principles that SSET must comply with:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed; and
- Processed in a way that ensures it is appropriately secure.

This policy sets out how SSET aims to comply with these principles.

7 Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8 Students

We process medical and health data for the purposes of assessing our ability to offer a potential student the necessary level of care and thereafter, meeting the needs of students at SSET, administering medical treatment and for use in medical emergencies.

9 Sharing personal data

We will not normally share personal information with anyone else, but may do so where:

- There is an issue with a student, resident, visitor, volunteer or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal information with law enforcement and government bodies where we are legally required to do so, including for:

- Where the disclosure is required to satisfy our safeguarding obligations;
- Where the disclosure is required to satisfy our contractual and/or legal obligations;
- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal information with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students, residents, volunteers or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

If particularly sensitive information is being shared via email, guidance is provided within the Acceptable Use of IT Policy to ensure information remains secure.

10 Privacy notices

SSET will issue Privacy Notices from time to time, informing individuals about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Students / Supported Living Residents and subject access requests

The basic rule is that personal information belongs to the individual.

SSET will often rely on parental consent to process information relating to students (if consent is required) unless it is more appropriate to rely on the student's consent. Parents should be aware that in such circumstances they may not be consulted on the request or receipt of consent from the child/young adult – although this will ultimately depend on the age, maturity and understanding of the child/young adult, the interests of the child/young adult, the parents' rights at law and all the circumstances.

In the case of Data Subject Access Requests in respect of a student's information, if the child/young adult is of sufficient age and maturity, they may be able to make a request in their own right. Alternatively, they may need to provide their parent or carer with the relevant consent for a request to be made on the child's/young adult's behalf.

It is accepted that most subject access requests for students and supported living residents at SSET will be made by parents or carers and these may be dealt with without the express permission of the student or resident. Matters should always be judged on a case-by-case basis.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12 Data protection impact assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where SSET is planning to use a new form of technology), we will, where necessary and before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the staff responsible should contact the DPL to assess whether a DPIA is required.

During the course of any DPIA, SSET will seek the advice of the DPL and, where appropriate, the views of affected individuals.

13 CCTV

SSET uses CCTV in various locations around the site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. When deployed, security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPL. Please refer to the SSET CCTV Policy for further information.

14 Photographs and videos

As part of SSET activities, we may take photographs and record images of individuals on devices approved and issued by SSET.

SSET uses images of students for four broad purposes:

- educational;
- marketing and promotional;
- to communicate with parents/carers and students; and
- for identification and security.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Uses may include:

- Within SSET on notice boards, brochures and newsletters;
- Outside of SSET such as in newspapers, campaigns; and/or
- Online on our SSET website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not use in future publications, although any use of the information whilst consent was in place is deemed to be valid.

When using photographs and videos in this way we will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

See our Safeguarding, Child Protection and Adults at Risk Policy along with our Acceptable use of IT Policy for more information on our use of photographs and images.

15 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitable DPL;
- Only processing personal information that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see paragraph 6 above);
- Completing privacy impact assessments where SSET's processing of personal information presents a high risk to rights and freedoms of individuals, and when introducing new technologies;
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Data Protection training is mandatory for all staff and is included within the induction programme for new staff. Update/refresher training is also mandatory, covering data protection law, this policy, any related policies and any other data protection matters; a record of attendance is maintained;
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Regularly conducting reviews to test our privacy measures and make sure we are compliant; and
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our DPL and all information we are required to share about how we use and process their personal data (via our Privacy Notices); and
    - For all personal information that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the information, retention periods and how we are keeping the information secure.

16 Data security and storage of records

SSET will protect personal information and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and protect against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept securely when not in use/ where possible locked away;
- Papers containing confidential personal information must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Passwords that are at least 8 characters long containing letters and numbers are used to access SSET computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals;
- Staff login credentials give access to a range of resources that include Internet, a range of educational and office-based software, and email. Staff can access network drives and folders. The level of information staff can access is controlled and will depend on job role;
- Encryption software is used to protect all portable devices and removable media, such as laptops; and
- Further details regarding data security of electronic records and devices can be found via our Online Safety Policy, Acceptable Use of IT Policy and 'UK GDPR & destruction of digital data – guidance', Appendix 2.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Where SSET uses external organisations (or third parties) to process personal information on its behalf (so that those organisations are processors as defined in applicable data protection laws),

additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of SSET;
- those processing the information are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-processors are only engaged with the prior consent of SSET and under a written contract;
- the organisation will assist SSET in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist SSET in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to SSET as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide SSET with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell SSET immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the DPL.

17 Disposal of records

Personal data that is no longer required will be disposed of securely.

Personal information that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. This is the responsibility of individual departments and their team members.

We will shred paper-based records either directly or using a third party to safely dispose of records on SSET's behalf requiring them to provide sufficient guarantees that it complies with data protection law. Confidential waste bins are located centrally in houses and admin offices.

Digital information will be deleted or over-written in accordance with the guidance provided in Appendix 2, 'UK GDPR and destruction of digital data – guidance'.

18 Personal data breaches

SSET will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a data breach, we will follow the Data Breach Procedure.

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- a non-anonymised dataset being published on the SSET website containing medical details;
- safeguarding information being made available to an unauthorised person;
- the theft of an SSET laptop containing non-encrypted personal data about students;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and/or
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

Where appropriate SSET will make the required report of a data breach to the ICO, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

19 Training and failure to comply

All staff and trustees are provided with data protection training as part of their induction process.

Data protection will also form part of regular mandatory training (minimum of every two years), and more frequently where changes to legislation, guidance or the SSET's processes make it necessary.

Failure to comply with this policy or to abide by training may lead to disciplinary action under our procedures, and this action may result in dismissal of staff for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

20 Monitoring arrangements

The DPL is responsible for monitoring and reviewing this policy.

this policy will be reviewed **every 2 years** (or as required in response to changes in legislation or practice) and shared with the Board of Trustees.

21 Links with other policies

Please refer to SSET's data protection Privacy Notices and, where appropriate, to its other relevant policies which contain further information regarding the protection of personal information in those contexts, including:

- Safeguarding, Child Protection and Adults at Risk Policy
- Online Safety Policy
- Acceptable Use of IT Policy (including internet, email and communications)
- Data Retention Policy/Schedules
- Employment related policies (including criminal record information)