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

IJ DATA PROTECTION POLICY

Reviewed: Senior Management Team, July 2020 (Every 2 years)
Ratified by Board of Trustees: August 2020
Full Review date: July 2022
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.

Contents

Introduction

This policy gives everyone within the SSET community important information about:

- the data protection principles with which SSET must comply;
- what is meant by personal information and sensitive personal information (also known as special category data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- individuals' rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

1 Aims

The Sheiling Special Education Trust ("SSET"/"we") aims to ensure that all personal information collected about staff, students, residents, parents, trustees, volunteers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and other relevant data protection legislation, including the Data Protection Act 2018 (DPA 2018).

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to individuals. Its purpose is to ensure that the rules are applied to all processing by SSET of all personal information, regardless of whether it is in paper or electronic format.

SSET obtains, keeps and uses personal information about individuals including its students, parents, family members, next of kin, trustees and staff (including job applicants, current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices) for a number of specific lawful purposes, as set out in SSET's data protection Privacy Notices.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information and how (and when) we delete that information once it is no longer required.

2 Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the relevant ICO codes of practice, for example, in relation to subject access requests.

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual who can be identified (directly or indirectly) from that information. 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 also known as sensitive personal data or information and needs additional protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics information • Biometric information • Health – physical or mental • Sex life or sexual orientation
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.
Pseudonymisation	The process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
Criminal records information	Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

4 The data controller

4.1 SSET processes personal information relating to parents, students, staff, trustees, visitors and others, and is the data controller for the purposes of data protection.

4.2 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

5.1 This policy applies to **all staff** employed by SSET. Staff members who do not comply with this policy may face disciplinary action. External organisations and individuals working on our behalf are expected to comply with this policy.

Board of Trustees

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

Data Protection Lead

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

5.3.1 overseeing the implementation of this policy;

5.3.2 monitoring our compliance with data protection law;

5.3.3 advising SSET and its staff on its data protection obligations; and

5.3.4 developing related policies and guidelines, where applicable. To this end, and where appropriate, the DPL will take professional advice and guidance.

5.4 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.

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

All staff

5.6 Staff are responsible for:

5.6.1 Collecting, storing and processing any personal data in accordance with this policy;

5.6.2 Informing SSET of any changes to their personal data, such as a change of address;

5.7 Contacting the DPL in the following circumstances:

5.7.1 With any concerns about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;

5.7.2 If they have any concerns that this policy is not being followed;

5.7.3 If they are unsure whether or not they have a lawful basis to use personal data in a particular way;

5.7.4 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 European Economic Area;

5.7.5 If there has been a data breach. See the Data Breach Procedure at Appendix 1;

5.7.6 Whenever they are engaging in a new activity that may affect the privacy rights of individuals;

5.7.7 If they need help with any contracts or sharing personal data with third parties.

6 Data protection principles

6.1 SSET must comply with the data protection principles, which state that personal data must be:

6.1.1 Processed lawfully, fairly and in a transparent manner;

6.1.2 Collected for specified, explicit and legitimate purposes;

6.1.3 Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;

6.1.4 Accurate and, where necessary, kept up to date;

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

6.1.6 Processed in a way that ensures it is appropriately secure.

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

6.3 To the extent that we process special category/criminal offence information (including in relation to health, racial or ethnic origin, religious or philosophical beliefs, special educational needs or safeguarding), we process this information in compliance with the data protection principles and for each type of data, we identify a lawful condition for processing set out in Article 9 of the GDPR and the Data Protection Act 2018.

7 Collecting personal data

Basis for processing personal data

7.1 In relation to any processing activity we will, before the processing starts for the first time (if it has not already started), and then regularly while it continues:

7.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the individual has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which SSET is subject;

(d) that the processing is necessary for the protection of the vital interests of the individual or another natural person;

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority;

(f) that the processing is necessary for the purposes of legitimate interests of SSET or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual — see clause 7.2 below.

7.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

7.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

7.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices;

7.1.5 where sensitive personal information is processed, also identify a condition for processing that information (see paragraph 8.2.2 below), and document it; and

7.1.6 where criminal offence information is processed, also identify a condition for processing that information (see paragraph 11.2.2 below), and document it.

7.2 When determining whether SSET's legitimate interests are the most appropriate basis for lawful processing, we will:

7.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

7.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

7.2.3 keep the LIA under review, and repeat it if circumstances change; and

7.2.4 include information about our legitimate interests in our relevant privacy notice(s).

8 Sensitive personal information

8.1 SSET may from time to time need to process sensitive personal information.

8.2 We will only process sensitive personal information if:

8.2.1 we have a lawful basis for doing so as set out in paragraph 7.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with SSET's legal obligations or for the purposes of SSET's legitimate interests; and

8.2.2 one of the conditions for processing sensitive personal information applies, e.g.:

(a) the individual has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of SSET or the individual;

(c) the processing is necessary to protect the individual's vital interests, and the individual is physically incapable of giving consent;

(d) processing relates to personal information which is manifestly made public by the individual;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

8.2.3 The SSET's data protection Privacy Notices set out the types of sensitive personal information that SSET processes, what it is used for and the lawful basis for the processing.

8.2.4 Before processing any sensitive personal information of a type or for a purpose not referred to in the SSET's data protection Privacy Notice, staff must notify the DPL of the proposed processing, in order that the DPL may assess whether the processing complies with the criteria noted above.

8.2.5 Processing of sensitive personal information of a type or for a purpose not referred to in SSET's Privacy Notices will not occur until:

(a) the assessment referred to in paragraph 8.2.4 has taken place; and

(b) the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

8.2.6 SSET will not carry out automated decision-making based on any individual's sensitive personal information.

8.2.7 In relation to sensitive personal information, SSET's procedures to ensure compliance with the data protection principles set out in paragraph 6 above include the following set out in paragraphs 10 to 12 below.

9 Limitation, minimisation and accuracy

9.1 We will only collect personal information for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their information – usually in the form of a Privacy Notice.

9.2 If we want to use personal information 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.

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

9.4 When staff no longer need the personal information they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the SSET's retention schedule.

10 Staff

10.1 **During the recruitment process**: we do not (except where the law permits otherwise):

10.1.1 Ask for sensitive personal information e.g. relating to race and ethnic origin, trade union membership and health during the short-listing, interview or decision-making stages;

10.1.2 if sensitive personal information is volunteered, no record is kept of it and any reference to it is immediately deleted or redacted;

10.1.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and will not be seen by the person shortlisting, interviewing or making the recruitment decision;

10.1.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

10.1.5 we will only ask health questions once an offer of employment has been made.

These purposes are consistent with the employment condition referred to in DPA, Schedule 1, paragraph 1 and the equality of opportunity or treatment condition in DPA, Schedule 1, paragraph 8.

10.2 **During employment**: we will process:

10.2.1 health information and disability status for the purposes of administering sick pay, assessing your fitness to work, providing workplace adjustments, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

10.2.2 details of individual's sex and sexual orientation for the purposes of administering family-related leave; and

10.2.3 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and

10.2.4 trade union membership information for the purposes of staff administration.

These purposes are consistent with the employment condition referred to in Data Protection Act 2018, Schedule 1, paragraph 1.

10.3 Staff members are required to take particular care in relation to their processing of sensitive personal information.

10.4 All sensitive personal information must be retained and disposed of in accordance with SSET's specified retention periods.

11 Criminal records information

11.1 We process criminal records information about staff, and volunteers to comply with our legal obligations.

11.2 We will only process criminal records information if:

11.2.1 we have a lawful basis for doing so e.g. to comply with SSET's legal obligations, where it is necessary for the purposes of SSET's legitimate interests; and

11.2.2 one of the conditions for processing criminal records in GDPR article 9 or DPA, Schedule 1 applies, e.g.:

(a) the individual has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of SSET or the individual;

(c) processing relates to personal information which are manifestly made public by the individual;

(d) the processing is necessary for the establishment, exercise or defence of legal claims; or

(e) the processing is necessary for reasons of substantial public interest.

11.3 SSET's Privacy Notices describe SSET's processing of criminal records information, what it is used for and the lawful basis for the processing.

11.4 Before processing any criminal records information for a purpose not referred to in SSET's Privacy Notice, staff must notify the DPL of the proposed processing, in order that the DPL may assess whether the processing complies with the criteria noted above.

11.5 Processing of criminal records information for a purpose not referred to in SSET's Privacy Notices will not occur until:

11.5.1 the assessment referred to in paragraph 11.4 has taken place; and

11.5.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

11.6 SSET will not carry out automated decision-making based on any individual's criminal records information.

11.7 Staff members are required to take particular care in relation to their processing of criminal records information.

11.8 All criminal records information must be retained and disposed of in accordance SSET's specified retention periods.

12 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. We process race/ethnicity information in order to monitor any achievement gaps across protect characteristics and fulfil our legal obligation to provide this data to OFSTED.

13 Sharing personal information

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

13.1.1 There is an issue with a student, resident, visitor, volunteer or parent/carer that puts the safety of our staff at risk;

13.1.2 We need to liaise with other agencies – we will seek consent as necessary before doing this unless there are legal reasons as to why we must share the information;

13.1.3 Our suppliers or contractors need information to enable us to provide services to our staff, students and residents – for example, IT companies. When doing this, we will:

(a) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

(b) Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal information we share

(c) Only share information that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

13.2.1 Where the disclosure is required to satisfy our safeguarding obligations;

13.2.2 Where the disclosure is required to satisfy our contractual and/or legal obligations;

13.2.3 The prevention or detection of crime and/or fraud;

13.2.4 The apprehension or prosecution of offenders;

13.2.5 The assessment or collection of tax owed to HMRC;

13.2.6 In connection with legal proceedings;

13.2.7 Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

13.3 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.

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

14 Privacy notices

14.1 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.

14.2 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.

14.3 Guidance on students' confidentiality can now be found at Appendix 3.

15 Data protection impact assessments (DPIAs)

15.1 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:

15.1.1 whether the processing is necessary and proportionate in relation to its purpose;

15.1.2 the risks to individuals; and

15.1.3 what measures can be put in place to address those risks and protect personal information.

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

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

16 Individual rights

16.1 Individuals have the following rights in relation to their personal information:

16.1.1 to be informed about how, why and on what basis that information is processed — see SSET's data protection privacy notices;

16.1.2 to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request;

16.1.3 to have personal information corrected if it is inaccurate or incomplete;

16.1.4 to have personal information erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

16.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where SSET no longer needs the personal information but the individual requires the information to establish, exercise or defend a legal claim; and

16.1.6 to restrict the processing of personal information temporarily where they do not think it is accurate (and SSET is verifying whether it is accurate), or where they have objected to the processing (and SSET is considering whether its legitimate interests override the individual's interests).

16.2 Individuals wishing to exercise any of the rights listed will be invited in SSET's Privacy Notices to contact the DPL. Any staff member who receives a request from an individual to exercise these rights must immediately refer it to the DPL.

Subject access requests

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

16.3.1 Confirmation that their personal information is being processed;

16.3.2 Access to a copy of the information;

16.3.3 The purposes of the information processing;

16.3.4 The categories of personal information concerned;

16.3.5 Who the information has been, or will be, shared with;

16.3.6 How long the information will be stored for, or if this isn't possible, the criteria used to determine this period;

16.3.7 The source of the information, if not the individual; and

16.3.8 Whether any automated decision-making is being applied to their information, and what the significance and consequences of this might be for the individual.

16.4 Subject access requests must be submitted in writing, either by letter or email to the DPL – highlighting the fact it is a 'subject access request'. They should include:

16.4.1 Name of individual;

16.4.2 Correspondence address;

16.4.3 Contact number and email address; and

16.4.4 Details of the information requested.

16.5 If staff receive a subject access request they must not respond themselves but immediately forward it to the DPL.

Students / Supported Living Residents and subject access requests

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

16.7 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.

16.8 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.

16.9 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.

Responding to subject access requests

16.10 When responding to requests, we:

16.10.1 May ask the individual to provide 2 forms of identification;

16.10.2 May contact the individual via phone to confirm the request was made;

16.10.3 Will respond without delay and within 1 month of receipt of the request;

16.10.4 Will provide the information free of charge; and

16.10.5 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.

16.11 We are obliged to comply with relevant data protection, safeguarding and other laws. SSET will assess whether it is able to disclose the information requested and will not disclose information if it:

16.11.1 Would involve disclosing information relating to another individual or third party;

16.11.2 Would reveal that the student is at risk of abuse, where the disclosure of that information would not be in the student's best interests;

16.11.3 Might cause serious harm to the physical or mental health of the student or another individual; and/or

16.11.4 Is the subject of legal professional privilege.

16.12 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

16.13 A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

16.14 If we refuse to deal with a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

17 CCTV

17.1 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.

17.2 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.

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

18 Photographs and videos

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

18.2 SSET uses images of students for four broad purposes:

18.2.1 educational;

18.2.2 marketing and promotional;

18.2.3 to communicate with parents/carers and students; and

18.2.4 for identification and security.

18.3 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.

18.4 Uses may include:

18.4.1 Within SSET on notice boards, brochures and newsletters;

18.4.2 Outside of SSET such as in newspapers, campaigns; and/or

18.4.3 Online on our SSET website or social media pages.

18.5 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.

18.6 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.

18.7 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.

19 Data protection by design and default

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

19.1.1 Appointing a suitable DPL;

19.1.2 Only processing personal informationthat 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);

19.1.3 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;

19.1.4 Integrating data protection into internal documents including this policy, any related policies and privacy notices;

19.1.5 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;

19.1.6 Regularly conducting reviews to test our privacy measures and make sure we are compliant; and

19.1.7 Maintaining records of our processing activities, including:

(a) 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

(b) 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.

20 Data security

20.1 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.

20.2 These may include:

20.2.1 making sure that, where possible, personal information is pseudonymised or encrypted;

20.2.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

20.2.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

20.2.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

20.3 In particular:

20.3.1 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;

20.3.2 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;

20.3.3 Where personal information needs to be taken off site, staff must consider the necessity and the risks involved based on the type of information. If no other workable alternative then staff must agree with their immediate line manager in advance and operate in line with any relevant policies and procedures;

20.3.4 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;

20.3.5 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;

20.3.6 Encryption software is used to protect all portable devices and removable media, such as laptops; and

20.3.7 Further details regarding data security of electronic records and devices can be found via our Online Safety Policy, Acceptable Use of IT Policy and 'GDPR & destruction of digital data – guidance', Appendix 2.

20.4 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:

20.4.1 the organisation may act only on the written instructions of SSET;

20.4.2 those processing the information are subject to a duty of confidence;

20.4.3 appropriate measures are taken to ensure the security of processing;

20.4.4 sub-processors are only engaged with the prior consent of SSET and under a written contract;

20.4.5 the organisation will assist SSET in providing subject access and allowing individuals to exercise their rights in relation to data protection;

20.4.6 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;

20.4.7 the organisation will delete or return all personal information to SSET as requested at the end of the contract; and

20.4.8 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.

20.5 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.

21 Storage, Retention and Disposal of records

21.1 Personal information (and sensitive personal information and criminal records information) will be kept securely.

21.2 Personal information (and sensitive personal information and criminal records information) should not be retained for any longer than necessary. The length of time over which information should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

21.3 Staff must adhere to SSET's specified retention periods, which are contained in the Data Retention Schedules. Where there is any uncertainty, staff should consult the DPL.

21.4 Personal information (and sensitive personal information and criminal records information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

21.5 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.

21.6 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.

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

22 Personal data breaches

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

22.2 In the event of a data breach, we will follow the procedure set out in Appendix 1.

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

22.3.1 loss or theft of data or equipment on which personal information is stored;

22.3.2 unauthorised access to or use of personal information either by a member of staff or third party;

22.3.3 a non-anonymised dataset being published on the SSET website containing medical details;

22.3.4 safeguarding information being made available to an unauthorised person;

22.3.5 the theft of an SSET laptop containing non-encrypted personal data about students;

22.3.6 loss of data resulting from an equipment or systems (including hardware and software) failure;

22.3.7 human error, such as accidental deletion or alteration of data;

22.3.8 unforeseen circumstances, such as a fire or flood;

22.3.9 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and/or

22.3.10 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

22.4 SSET will:

22.4.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, 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

22.4.2 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.

23 Training and failure to comply

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

23.2 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.

23.3 Staff members are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

23.4 SSET takes compliance with this policy very seriously. Failure to comply with the policy:

23.4.1 puts at risk the individuals whose personal information is being processed; and

23.4.2 carries the risk of significant civil and criminal sanctions for the individual and SSET; and

23.4.3 may, in some circumstances, amount to a criminal offence by the individual.

23.5 Because of the importance of this policy, failure to comply with any requirement of it 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.

24 Monitoring arrangements

24.1 The DPL is responsible for monitoring and reviewing this policy.

24.2 This policy will be reviewed and updated as required in line with significant changes in Data Protection Law that affect SSET's practice. Otherwise this policy will be reviewed **every 2 years** and shared with the Board of Trustees.

24.3 If you have any questions or comments about the content of this policy or if you need further information, you should contact the DPL (see paragraph 5.5 above).

25 International transfers

25.1 SSET will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

26 Links with other policies

26.1 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:

26.1.1 Safeguarding, Child Protection and Adults at Risk Policy

26.1.2 Online Safety Policy

26.1.3 Acceptable Use of IT Policy (including internet, email and communications)

26.1.4 Data Retention Policy/Schedules

26.1.5 Employment related policies (including criminal record information)

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1 On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPL. Depending on circumstances the DPL will investigate or will put together a small team from SSET senior managers to investigate.

2 The DPL and team will investigate and determine whether a breach has occurred, taking professional advice as required. To decide, the DPL and team will consider whether personal data has been accidentally or unlawfully:

- **(a)** Lost
- **(b)** Stolen
- **(c)** Destroyed
- **(d)** Altered
- **(e)** Disclosed or made available where it should not have been
- **(f)** Made available to unauthorised people

3 The DPL will alert the principal and the chair of trustees

4 The DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

5 The DPL and team will assess the potential consequences, based on how serious they are, and how likely they are to happen

6 The DPL and team will work out whether the breach must be reported to the ICO following any professional advice sought. This must be judged on a case-by-case basis. To decide, the DPL and team will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- **(a)** Loss of control over their data
- **(b)** Discrimination
- **(c)** Identify theft or fraud
- **(d)** Financial loss
- **(e)** Damage to reputation
- **(f)** Loss of confidentiality
- **(g)** Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPL must notify the ICO.

7 The DPL will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically by the DPL.

8 Where the ICO must be notified, the DPL will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPL will set out:

- **(a)** A description of the nature of the personal data breach including, where possible:

(b) The categories and approximate number of individuals concerned

(c) The categories and approximate number of personal data records concerned

(d) The name and contact details of the DPL

(e) A description of the likely consequences of the personal data breach

(f) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

9 If all the above details are not yet known, the DPL will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPL expects to have further information. The DPL will submit the remaining information as soon as possible.

10 The DPL and team will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPL will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

(a) The name and contact details of the DPL

(b) A description of the likely consequences of the personal data breach

(c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

11 The DPL will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

12 The DPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

(a) Facts and cause

(b) Effects

(c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

13 Records of all breaches will be stored on SSET's computer system by the DPL.

14 The DPL and principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Appendix 2: GDPR and destruction of digital data – guidance

SSET processes a range of personal data. The organisation acknowledges that much of our information is stored in a digital format. Various categories of information, in line with SSET's 'Retention Schedule', each have a defined retention period, after which such information must be securely archived or disposed of/ destroyed.

This guidance explains the various ways in which digital data is stored and how it is destroyed as it reaches the end of the retention period. SSET will take all practicable steps to ensure that digital data is securely destroyed. This means ensuring that the data is irrecoverable and cannot be deliberately or accidentally found by known conventional means.

Data stored on the SSET Network/ Server

The majority of data is stored on the server. Data generated or stored can be in a variety of network drives and these include Central Core (management or departmental data) and the individual employees U: Drive.

Data will be stored in a logical format on the server, to avoid replication. Individual departments will be responsible for ensuring the relevant data is deleted from network locations as it reaches the end of its retention period. The Head of Finance & Premises, Network Manager and Head of School will retain the right to monitor and inventory server content to ensure that data does not exceed the relevant retention period.

The data on the server is securely encrypted. When data is deleted from the server, it is no longer visible to connected computers as the link to the file no longer exists. The server completes regular backups. These overwrite the server contents. This means any file remnant from deletion is also overwritten.

Data stored on SSET computers

A 'computer' for the purpose of this guidance includes mobile devices such as laptops and tablets alongside desktop machines. Users may store data for business purposes on computers that belong to SSET. This is usually a temporary measure to work on a file, as published/ completed information goes to the Server or SharePoint. SSET computers such as laptops are also encrypted, making their data more secure.

All machines will be refreshed annually with all user data deleted. Again, deletion of files simply means the link to the file is removed. SSET will run proprietary software on an ongoing basis to clean up any free space on hard disk drives. This includes 3-pass deletion of any unused space including deleted files. This renders such data irrecoverable by any conventional known means.

Hosted data- DataBridge, SharePoint, SelectHR, Google Drive, iCloud, Classroom Monitor

SSET stores a range of data external to the site through reputable, established providers in the sector. All of these providers will have a responsibility to ensure that their management of client data is in line with Data Protection laws. For all providers, SSET will seek documentary evidence through written statement or policy that use is compliant with the relevant regulations. Where any data stored reaches the end of a retention period, SSET will use the providers' established method of deleting data. This usually involves deleting the relevant records or setting them to inactive, prior to deletion. Data security protocols will apply to all such resources, such as user account control, to ensure that only the appropriate staff can access any stored data.

IT Equipment

IT equipment that reaches the end of usable life will be destroyed. This means the hard drive will be destroyed, also. Equipment will be rendered inoperable and so that any data on the machine is inaccessible by any known conventional means.

Appendix 3 – Confidentiality

SSET supports the view that students' privacy and confidentiality will be respected and that information about them should be discretely handled, and that this should occur in a manner which is consistent with good practice and the need to protect the student.

1 Access to case records by staff and others:

1.1 Student's records will be kept safely and securely and the contents only shared with those who have a *bona fide* right and need to know their content in order to safeguard and protect the student's welfare. The storing and processing of personal information about students is governed by data protection law.

1.2 Staff are made aware that all files/records and their content required for working with students are confidential materials. These may **only** be obtained under appropriate authorisation including that of a senior house coordinator/teacher or therapist who will supervise their use.

1.3 Students wishing access to information/records/reports about themselves must discuss this with their House Managers. Requests will be considered on an individual basis and in line with the principles contained in this policy.

1.4 Students should be made aware of the content of reports/records as appropriate to their understanding and who has access to it within SSET. Some students would benefit from assisting in writing sections of their Individual Care Plans, and review updates and this should be considered on an individual basis.

2 Passing on of information with child protection implications is covered in our 'Safeguarding, Child Protection and Adult at Risk Policy'

Staff are familiar with the 'Safeguarding, Child Protection and Adult at Risk Policy' and will have the necessary training, qualifications and experience to know how to deal with and share information which they are given in confidence. The sharing of personal information may be necessary for reasons of the student's care, education and protection.

Phone calls, visits at SSET and use of phone.

2.1 Staff will safeguard the student's right to communicate with others by letter, telephone and e-mail without these being read by others.

2.2 They will respect the rights of privacy and confidentiality in situations where students will require support to communicate with others.

2.3 Information about services, such as helplines which students may wish to consult confidentially should be displayed on a house notice board, in a suitable format for easy access and adjacent to the telephone used by students for such private conversations.

2.4 SSET will provide a private space for the student to access the telephone cordless phone that can be taken into the bedroom.

2.5 Any restrictions on the use of phones should be with prior agreement of the parent or student representative and the Local Authority.

2.6 SSET will provide a space for the student to meet privately with their parent or representative.