SPECIALIST EDUCATION SERVICES

Data Protection Policy and Practice

Date created or revised: 0123
Date of next review: 0823

SES Avocet House Ltd (4926028), SES Turnstone House Ltd (7972485) and SES Kite Ltd (12634002) are subsidiary companies of Specialist Education Services Topco Ltd (13159680)

CONTENTS

1 INTRODUCTION

This policy governs the use of personal information within SES so that all staff, parents, children, young adults, contractors and other individuals will have a clear idea of the limits of use of personal information, and where to go for further advice.

1.1 PURPOSE

This policy lays down the principles for the processing of personal information, whether it relates to staff, suppliers, visitors, customers or others. Personal information means any information relating to a living, natural person, who can be identified either directly or indirectly. Processing personal information includes the obtaining, handling, processing, transporting, storing, destruction and disclosure of personal information.

It is not designed to replace practical advice from the Data Protection Officer. Nor is it intended to provide all the answers to questions concerning the use of personal information in particular areas, such as HR, IT or marketing.

Additional guidance notes on specific issues (e.g. Subject Access Rights) are also available from the relevant policy document.

1.2 SUMMARY

SES will use the personal information of individuals fairly, lawfully, transparently and in a manner consistent with its valid business interests and at the same time, respecting the fair and lawful privacy requirements of those individuals concerned.

1.3 STATUS OF POLICY

Staff who process personal information on behalf of SES must adhere to the terms of this policy and any breach will be taken seriously and may result in formal disciplinary action.

This policy should be read in conjunction with the following Policy and Practice documents:

- Communications
- Acceptable Use of Technology

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with a line manager or the Data Manager (currently the SES Principal). The Data Protection Officer is also available for advice.

Any staff who consider this policy has not been followed should raise this matter with their relevant manager within SES or (if an employee related issue) the SES Principal. If the matter is not resolved it should be raised as a formal grievance.

1.4 FURTHER ADVICE

Further advice may be obtained from your line manager, the Data Manager or the

Data Protection Officer who can be contacted at DPO@priviness.eu.

2 GOVERNING PRINCIPLES

2.1 DATA PROTECTION PRINCIPLES

Personal information will be used within SES by its staff according to the principles of applicable data protection legislation (the "DP Legislation"), meaning the General Data Protection Regulation (“GDPR”), the Data Protection Act (“DPA”) and the Privacy and Electronic Communications Regulations ("PECR"). The principles require that personal information will be:

2.1.1 Lawfulness, Fairness and Transparency

The DP Legislation seeks to ensure that processing is carried out lawfully, fairly and transparently without adversely affecting the freedoms, interests and rights of the individual concerned.

For personal information to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the individual data subject has consented to the processing, or that the processing is necessary for the performance of the contract with the individual, for compliance with a legal obligation, the vital interest of the data subject, or the legitimate interest of SES or the party to whom the information is disclosed.

DP Legislation imposes specific requirements in relation to electronic marketing (e.g. email, Apps, social media and SMS), telephone marketing and the use of tracking or profile analysis technology (e.g. to deliver targeted online advertising). It is very important to that staff seek advice from internal teams, including the Data Manager before undertaking such activities on behalf of SES. The Data Protection Officer is also available for advice.

Before personal information is passed to third parties, including law enforcement agencies, government bodies, investigators or anyone else, it is important that full consideration is made of the possible data protection implications of doing so. All staff should contact the Data Manager where there are questions or doubts regarding a particular request. The Data Protection Officer is also available for advice to the Data Manager.

2.1.2 Purpose Limitation

Personal information may only be processed for the specific purposes notified to the individual when the information was first collected or for any other purposes specifically permitted by the DP Legislation. This means that personal information must not be collected for one purpose and then used for another, unless the other purpose is also specified.

2.1.3 Data Minimisation

Only personal information that is necessary for the purposes specified should be collected. Any data which is not necessary for that purpose should not be collected in the first place.

2.1.4 Accuracy

Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information should be securely destroyed.

2.1.5 Storage Limitation

Personal information should not be kept longer than is necessary for the purpose for which it was collected. This means that data should be destroyed or erased from our systems when it is no longer required.

2.1.6 Integrity and Confidentiality

SES must ensure that appropriate safeguarding measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Individual data subjects may apply to the courts for compensation if they have suffered damage or distress from such a loss.

Tough new obligations to notify, in certain situations, regulators (and affected individuals) now exist if the above mentioned safeguarding measures fail to protect personal information. It is therefore very important that you immediately report any suspected incident to the Data Manager and the Data Protection Officer.

The DP Legislation requires SES to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction, be it paper-based or in electronic format.

Personal data may only be transferred to a third-party data processor (such as a supplier or service provider to SES or a group company) if they agree to comply with those procedures and policies, or if they put in place adequate measures. DP Legislation also requires SES to have a written contract in place with all suppliers or service providers who will process their personal information. It is therefore important that procurement are involved in all such arrangements, that the correct procurement templates are used and/or that internal legal teams are consulted prior to the engagement of suppliers and partners who will either process personal information per SES instructions or jointly process personal data.

2.1.7 Accountability

SES must ensure that we are able to evidence compliance with DP Legislation.

For example, that all the above principles have been applied, documentation is up to date, training on data protection and privacy has been completed, and security measures are complied with.

2.2 COMPLIANCE WITH THE PRINCIPLES

In order to meet the requirements of the principles SES will:

- observe the conditions regarding the fair, lawful and transparent collection and processing of personal information;
- meet its obligations to specify the purposes for which personal information is used;
- collect and process personal information only to the extent it is required for SES's valid business interests and where there is a legal basis for doing so;
- ensure the quality of the personal information used;
- adopt a data retention and disposal policy that includes the length of time personal information is held;
- ensure that the rights of individuals about whom personal information is held can be fully exercised under the respective DP Legislation;
- take appropriate technical and organisational safeguarding measures (which include strict Personnel access controls) to protect personal information including following the policy guidelines set out in SES IT Communications Policy and IT Acceptable Use of Technology Policy;
- ensure that any contractor, agent or other third party who processes personal information on SES's behalf does so under a written contract requiring that third party to:
    - only process the personal information in accordance with SES's instructions; and
    - take appropriate technical and organisational security measures to safeguard personal information; and
    - ensure that personal information is not transferred outside the European Economic Area without suitable safeguards; and
    - confirm destruction of all information. This should include paper, electronic and consideration should be given to backup media; and
    - which contains additional data processing clauses which are specified in the DP Legislation.

2.3 RESPONSIBILITY FOR COMPLIANCE

SES is a data controller (and, in certain circumstances, also a processor) responsible for complying with the DP Legislation.

It is the responsibility of each member of staff to comply with this policy when using personal information relating to team members, customers or others.

The Data Manager has responsibility for this policy and its review.

3 LEGAL BASIS

All processing must be lawful, which means that there must be one of the following legal grounds established before processing can take place:

3.1 CONSENT

When using consent, SES must be able to demonstrate that consent has been unequivocally given, not just implied. Consent cannot apply to children under 13 vis-à-vis online unless the holders of parental responsibility have provided it. Nor can consent be coerced, for example, forced consent as part of a contract. Consent is a valid legal basis for processing of special categories of personal information. Consent must be prominent in any privacy statement:

- freely given, specific, informed and unambiguous
- a clear affirmative action, signifying agreement to the processing of their personal information

When consent is given in the context of a statement which also concerns other matters, the request for consent needs to be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

When consent is provided, it must be able to be withdrawn at any time with as much ease as it was originally given. If withdrawn, the information must be erased. The right to data portability applies in the case of contract being the legal basis.

When carrying out any direct marketing using personal information SES will:

- only market to those individuals under the correct legal basis, such as consent, and for the specific purposes notified to the guest or customer when the personal information was collected;
- use safeguarding measures such as the Telephone Preference Service, Mailing Preference Service and other third party suppression lists where appropriate;
- use standard SES consent wording; and
- require third party partners to use an approach compatible with this document when capturing consents on SES's behalf.

Any use of personal information for direct marketing purposes which is not in accordance with the requirements set out above must be approved, in advance, by the Data Manager and Data Protection Officer.

An example of this legal basis is seeking adult and young person photgraphic consent for use of personal images in our SES brochures, other printed publications, for identity cards and the SES website.

3.2 LEGITIMATE INTERESTS

It is always important to demonstrate the necessity for SES to process personal information for its legitimate interests if relying on this legal basis.

When using legitimate interests, SES must be able to demonstrate that there are no over-riding risks to the individuals' interests, rights or freedoms.

Therefore, SES's legitimate interests when weighed up against the risks to individuals must always be taken into account when conducting a data protection impact assessment (required for any new system or process – or a significant change). Similarly, the mitigating measures that are applied need to be documented.

3.3 CONTRACT

When using contract as the legal basis, SES must be able to demonstrate that the necessity of the performance of a contract (or negotiation of a contract) with the individual, for example, employee, supplier or customer / guest.. The right to not being subject to automated decision-making, including profiling, does not apply where there is a necessity for the purposes and legal basis of a contract (or entering into a contract).

The right to data portability applies in the case of contract being the legal basis.

NB - Consent is presumed not to be freely given if it does not allow separate consent to be given if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance.

3.4 LEGAL OBLIGATION

When there is a statutory obligation, SES must be able to demonstrate for the specific purposes of processing personal information what that legal obligation is, third parties who receive the personal information under the auspices of the obligation, and any retention obligations required.

3.5 VITAL INTERESTS

When using vital interests, SES must be able to demonstrate that there is a necessity to process personal information in the vital interests of the individual concerned. For example, capturing allergy information when taking a table booking.

3.6 PUBLIC INTEREST

When using public interest, SES must be able to demonstrate that there is a need to store personal information in the interests of the public. For example, for public safety and security purposes, retaining staff information to pass to emergency services personnel given some event.

4 REQUIREMENTS

4.1 NOTICES

Individuals have the right to be informed regarding the specific purposes that their

personal information is being processed before processing takes place, for how long the information will be stored and processed, who it is being shared with (including internationally), and if there is automated decision-making, including profiling.

See appendices for more detail and an illustration of the SES standard Privacy Notice wording.

4.2 TRANSFERS

The DP Legislation prohibits us from transferring personal information to countries outside the European Economic Area (EEA), unless SES first put in place additional safeguards.

For example, before transferring information, SES may need to enter into contracts with recipients in non-EEA countries which incorporate Standard Contractual Clauses approved by the EU Commission.

Any such transfers should be notified to the Data Manager and Data Protection Officer stating who the data is being shared with, and if it is subject to any automated decision-making, including profiling.

4.3 RETENTION

In accordance with the principle of Data Minimization SES will hold data for no longer than is necessary for the original purpose for which the data was collected.

However, SES has a duty to retain some staff and child personal data for a significant period of time following their departure from the school and children's home, mainly for legal reasons, but also for other purposes such as being able to provide references.

Different categories of data will be retained for different periods of time.

4.4 DISPOSAL OF INFORMATION

Printed information will be shredded. Any computer or portable media containing information will be securely and permanently deleted and/or physically destroyed.

4.5 DATA PROTECTION BY DESIGN / DATA PROTECTION BY DEFAULT - APPROACH

SES ensures that policies reflect processes and a culture of respecting privacy. This includes ensuring that staff are accountable for the security and other safeguarding measures are adhered to, as well as collecting, processing storing, and only sharing it with those authorised and required to use it, only the personal information that is required, and only for as long as it is required for.

4.6 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIA guidance is to undertake an assessment from a risk-based perspective.

Any new process or system that includes innovative technologies or processing personal information or monitoring individuals on a large scale, where there is a higher risk to rights and freedoms of individuals affected.

5 DATA SUBJECT RIGHTS

5.1 SUMMARY OF RIGHTS

The subjects of personal information held by, or on behalf of, SES ("Data Subjects") have a wide range of rights granted to them under the DP Legislation. Whilst SES can make use of personal information for specific purposes and where we can lawfully justify such use, an individual can still exercise significant control over what SES do. SES need to operate as a business and process personal information in a way which facilitates the rights of individuals to exercise this control.

Today's DP Legislation significantly enhances the rights available to individuals. A summary of each of the rights is set out below.

It is important that requests from individuals wishing to exercise any of the rights below are quickly identified and sent to the appropriate person for preparing a response. Personnel should not respond to such requests without first discussing the matter with their line manager, who may refer the matter to the Data Manager. If required the Data Manager will liaise with the Data Protection Officer.

(See also SES Data Subject Rights Process Policy and Practice Document)

5.2 RIGHT TO BE INFORMED

Individuals have the right to be informed of how their personal information is being processed.

This must be provided in a privacy notice – the notice may be in the form of:

- a privacy statement or privacy policy, separate to a cookie policy (which is also required);
- an email signature, other correspondence, or information board in a public area;
- a privacy clause in an Employee Handbook; or
- a clause within the Terms and Conditions of a contract.

In general, individuals must be informed about:

- the purpose for processing their personal information,
- what information is processed, and
- for how long.

The notice should also include the contact details of SES and the Data Protection Officer.

Within the privacy notice, individuals also have the right to be informed whether any

third parties are to be recipients of their personal information.

Similarly in the same notice, individuals have the right to be informed whether their personal information will be transferred to 3rd countries or international organisations – generally outside the European Economic Area not covered by the 'adequacy' regime or other safeguards, such as Binding Corporate Rules or Standard Contract Clauses.

5.3 RIGHTS TO ACCESS (SUBJECT ACCESS REQUESTS)

Individuals have the right to request that SES:

- confirm, amongst other things, whether SES are holding their personal information;
- provide them with a copy of that information, and
- provide them with supporting (and detailed) explanatory materials.

SES must comply with Subject Access Requests without undue delay and at the latest within one month of the request (although this can be extended in limited circumstances), and cannot charge individuals for making a request (except in specific situations). Particular care should be taken if a request from one individual would result in personal information of another individual being disclosed (seek advice from the Data Manager and Data Protection Officer, about whether such information should be redacted or its disclosure justified).

Please contact the Data Manager and Data Protection Officer if you receive a request for the release of personal information.

5.4 RIGHT TO RECTIFICATION

Individuals have the right to require SES to rectify inaccuracies in personal data held about them. In some circumstances, if personal information records are incomplete or inconsistent, individuals have the right to require SES to complete the data, make it consistent, or to record a supplementary statement correcting it.

Advice should be sought from the Data Manager and Data Protection Officer if uncertain.

5.5 RIGHT TO ERASE (RIGHT TO BE FORGOTTEN)

Individuals have the right to have their personal information erased in certain specified situations – in essence where the continued processing of it does not comply with DP Legislation.

Where an individual makes an erasure request, SES must respond without undue delay and in any event within one month (although this can be extended in limited circumstances).

There are a number of exemptions which apply to such requests, and staff should not assume that SES should delete personal information simply because they have received a request of this nature.

Such a request should be referred to the Data Manager and Data Protection Officer as soon as it is received.

5.6 RIGHT TO RESTRICTION

This right allows individuals, in certain situations, to restrict use of their personal information. This might result in the use of it being limited to storage only, and could mean SES have to move personal information to separate IT systems, or temporarily block access to it.

This issue could arise in a situation where an individual is disputing the accuracy of information held, or where they are objecting to SES's right to continue to use their information and there is a need to take some time to establish whether we have a right to continue to do so.

Such a request should be referred to the Data Manager and Data Protection Officer as soon as it is received.

Advice should be sought from the Data Manager, who will liaise with the Data Protection Officer if uncertain.

5.7 RIGHT TO DATA PORTABILITY

Data portability goes beyond rights of access and requires SES to provide, on request, information to individuals in a structured, commonly used and machine-readable format. SES could also be asked by an individual to transmit personal information directly to another data controller in the same format.

This right only applies to electronic records which have been provided to SES by the individual themselves, or generated from their activity or observations of their activity (but not subsequent analysis of such activity), and only where SES hold the personal information because the company have the individual's consent or because of fulfilling a contract with them.

Such a request should be referred to the Data Manager and Data Protection Officer as soon as it is received.

5.8 RIGHT TO OBJECT

Individuals have an absolute right to object to their personal information being processed for the purpose of direct marketing. If SES receive any such objection we must immediately cease such marketing activities in respect of that individual.

Individuals have a wider right to object to processing undertaken which is justified on the basis that it is in SES's legitimate interests (rather than because SES have their consent). If SES receive an objection of this nature the company must assess the objection and carefully consider if SES can demonstrate compelling legal grounds to continue to process the personal information.

Such a request should be referred to the Data Manager and Data Protection Officer as soon as it is received.

5.9 RIGHTS IN RELATION TO AUTOMATED DECISION MAKING, INCLUDING PROFILING

Individuals have rights which apply if SES take decisions about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on the individuals. An example of this would be the use of an algorithm to analyse alumni data and decide which groups of people receive preferential promotional offers.

SES can use such automated decision making in circumstances where there is a need to do so in order for SES to enter into a contract with the individual, or where SES have their explicit consent. However, SES need to be transparent with individuals about what decisions are taken in this way, and SES may need to put in place additional protective measures to protect the individuals concerned.

Such a request should be referred to the Data Manager and Data Protection Officer as soon as it is received.

5.10 RIGHT TO COMPLAIN

Individuals have the right to bring a complaint to the Information Commissioner, or other supervisory authority.

5.11 RIGHT TO BRING LEGAL PROCEEDINGS

Individuals have the right to seek judicial remedy through the Courts.

5.12 REQUESTS

Staff, students, alumni and other subjects of personal information held by, or on behalf of SES may exercise any of the rights specified above. These rights are subject to certain exemptions which are set out in the DP Legislation.

Any staff member, student, alumni or other subject of personal information wishing to exercise any of these rights should make the request in writing to the Data Manager and Data Protection Officer.

SES aims to comply with any requests in relation to personal information as quickly as possible and in any event within the time specified by DP Legislation.

6 STAFF RESPONSIBILITIES

6.1 STAFF RESPONSIBILITIES FOR THEIR OWN DATA

All staff are responsible for:

- checking any personal information which they provide to SES is accurate and up to date;
- informing SES of any changes to personal information which they have provided, for example change of address; and

- checking any information that SES may send out from time to time, for example giving details of personal information that is held by SES.

6.2 RESPONSIBILITIES FOR OTHER DATA

If, as part of their responsibilities, staff have access to or use personal information about other people as part of their employment duties (for example, customer or guest personal information) they must comply with this policy and in SES's other policies and procedures for processing personal information (most notably the SES Acceptable Use of Technology policy).

As an individual you are responsible for ensuring that:

- Any personal data that you hold is kept securely
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party
- Personal information is not transferred internationally without checking first that the right safeguards are in place.
- You avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be locked out of sight
- Passwords and logon information are not disclosed to anyone else
- Personal information is kept in a locked filing cabinet, or in a locked drawer, or
- If it is computerised, be password protected
- If kept temporarily on portable media be password protected, encrypted and kept securely, having been first discussed with the data manager
- Login passwords are changed when requested to do so by the data manager and in line with issued guidelines for password suitability
- If you are aware of a breach of security with passwords or logon information the SES Principal / Deputy Principal, Registered Manager, Head of Education or Young Adult Residential Support Manager is informed immediately

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. In particular any **deliberate** or **serious** breach of this Data Protection Policy by a member of staff may lead to dismissal and even to criminal prosecution.

6.3 ACCESS RESTRICTION

Only those staff who strictly require access to personal information for their role should have such access, and all staff must make sure that personal information is not shared with adults who do not need to see it.

6.4 SPECIAL CATEGORIES

Personal information about staff and others may include special categories of personal information or other information that needs to be treated sensitively. This is personal information relating to an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;

- membership of a trade union;
- physical or mental health or condition;
- sexual life;
- sexual orientation;
- biometric or genetic data (e.g. facial or iris imaging, or biological sample information.)
- commission or alleged commission of an offence;
- any proceedings for any offence or alleged offence, the disposal of such proceedings or any sentence imposed by a court

Particular care must be taken when dealing with any personal information falling under one or more of these headings. If in doubt, do take advice from the Data Manager and Data Protection Officer. In general, such personal information must be kept very secure and must only be allowed to be seen by a restricted number of people who need to know it. The Data Protection Officer will act as an intermediary between SES, employees, suppliers, customers, partners and others.

7 EMAIL AND ELECTRONIC COMMUNCIATION

Due to the ease with which large quantities of personal data can be accidentally or inappropriately exposed when using email staff should be particularly careful to use email in a considered manner. In particular:

- Emails sent using the supplied '@specialisteducation.co.uk' domain are encrypted through the Office 365 system.
- External recipients of emails from '@specialisteducation.co.uk' domain can access messages via their own Microsoft 365 account, or by a one time passcode.
- If using an encrypted email attachment to send personal data do not include the password in the same email and preferably use a different communication method to send the password
- Emails sent from "@specialisteducation.co.uk" addresses to "@specialisteducation.co.uk" addresses are restricted to the secure environment and may include personal data
- Do not include any personal information in the "Subject" field of email regardless of the recipient, in particular do not include child's names or other potential identifiers.
- Staff should make it a habit to preferentially use "Bcc" rather than "Cc", "Cc" should only be used where it is necessary for all recipients to see replies.
- When using Distribution Lists to send emails to those outside SES, ensure that email addresses are not shared. Use the "Bcc" facility so that email addresses are not displayed.

Staff are permitted to use What's App for immediate communication between team members. Parameters are set for staff to follow, for further details please see the SES Acceptable Use of Technology Policy.

8 DBS CHECKS

Agreement to SES processing certain types of personal data is a condition of employment for staff.

This includes information about previous criminal convictions.

All members of staff and volunteers who come into contact with children or vulnerable young adults will be subject to Enhanced DBS checks. SES has a duty under the Children Act, Health and Social Care Act and other enactments to ensure that staff are suitable for the job.

We also have a duty of care to all staff and volunteers, and must, therefore, make sure that employees and those who use SES facilities do not pose a threat or danger to other users.

9 MEDICAL INFORMATION

SES will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes.

SES will only use the information in the protection of the health and safety of the individual.

10 AUDIT

At the beginning of each financial year, SES shall undertake a data protection audit to benchmark year-on-year compliance and improvement.

11 APPENDICES

A Organisational Technological Measures
B Privacy Notices
C Appropriate Policy Document

APPENDIX A

Organisational Technological Measures

SES SERVERS

Both Avocet House and Turnstone House have NAS drives functioning as 'servers', located in the main administration offices. Each office is fully alarmed overnight and for any extended periods when not occupied by the staff, e.g. weekends.

Each server has two separate backups, both of which are encrypted. On each site, the backups are located in different buildings to maximise the protection of SES data.

KERIO

The Kerio Control Box is a UTM (Unified Threat Management) appliance that integrates Kerio's award winning Kerio Control software with specially matched hardware to create a complete network security solution for small and medium sized organizations. It is a complete Network Firewall, Router and IPS (Intrusion Prevention System). It also has built in Web and Content filtering with logging and a built in secure VPN, although this is not in use currently.

COMPANY EMAIL

All SES email is hosted with Office 365, employing encryption for all communication. Multiple layers of encryption are in place at the same time. With Office 365, SES data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).

PORTABLE LAPTOPS

All staff are supplied with a laptop for personal, work related use and to gain access to the SES network. They are the prime method of communication (via email) in the 24/7 pace of rotational shift patterns. They are provided as a means of enabling colleagues to work more effectively and efficiently.

Staff adhere to guidelines within the Acceptable Use of Technology Policy and Practice Document. All laptop hard drives should be encrypted using Apple FileVault. Additionally, if an adult needs to leave their computer unattended temporarily whilst working, the screen saver (display lock) must be activated. Password management requires that each member of staff update their user login password for their laptop at least twice a year.

When using their laptop at home or away from the workplace, staff must follow the same high security standards. Laptops must be kept out of sight and securely in the boot of a car during transit. If left unattended in the home staff must be aware of the risk of family and friends accessing sensitive data, and therefore must take adequate measures to maintain security (Staff are issued with a DPIA for Working From Home each time this policy is reviewed and issued).

PASSWORD MANAGEMENT

Staff and young people are allocated passwords for the following technological services:

Kerio	Access to SES internet is password protected. No guest access is available. All staff have individual passwords that are not disclosed to any other parties.
Network	Staff access to SES network (server) is password protected. The Kerio and network passwords are different.
Emails	An email password is automatically set for staff by the system administrator. The email password is highly complex and can only be reset by the system administrator.
Screen lock	All staff must use a screen lock password for their laptop, that is updated twice per year as a minimum requirement. The screen lock must be activated whenever their laptop or workstation is unattended.
Wifi	SES wifi access is protected by a strong password only made available to the Principal and other designated senior leaders.
Clearcare	Staff access to Clearcare is password protected; the password must be changed every 90 days by staff (this function is automated by Clearcare).

The System Administrator (currently Osiris IT) maintains a secure list of all passwords for the various access required at SES establishments. A Controller – Processor signed agreement for data protection is in place with the system administrator.

CYBER INSURANCE

SES have authorised cyber insurance to protect the company. The policy provides comprehensive cover protection for: Cyber Incident Response, Cyber Crime, System Damage and Business Interruption, Network Security and Privacy Liability, Media Liability, Technology Errors and Omissions and Court Attendance Costs.

APPENDIX B

SES Privacy Notices

Privacy notices are in place for:

- SES Employees
- Parents, Guardians, Family Members
- Point of Contact Referees
- Professional Services
- Recruitment Candidate
- SES Website user

The SES Employee privacy notice is included as an example; others are available via the administration teams.

Data Subject: Employee

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Specialist Education Services
The Old Vicarage
School Lane
Heckingham
Norfolk
NR14 6QP

For queries to this notice please contact or Data Protection Officer at – dpo@priviness.eu

As an employee of Specialist Education Services, we hold the following information about you:

- personal information such as name, gender, date of birth, dependants, next of kin, job title, NHS number
- contact details such as addresses, telephone numbers, email addresses and emergency contact details.
- identification information such as photographs, video clips, passport and/or driving licence details, etc.
- pay and financial information such as salary, benefits (including pensions), bank account details, card details, timesheets, National Insurance number.
- recruitment and professional information such as application forms, CVs, academic and training-related information, records/results of any pre-employment checks, references.
- employment and management records such as disciplinary and grievance records, flexible working requests, performance records, appraisals and training records, holiday and attendance records.
- right to work documentation such as proof of eligibility to work in the UK and obtaining and maintenance of any necessary professional consents or licences.

- information relating to access to our premises and/or use of our management and IT systems such as system ID, passwords, use of websites, emails sent or received, telephone calls, entry/exit records.

We also handle the following special categories of sensitive personal information:

- any trade union memberships you hold, information about physical and mental health, including any medical conditions, biometric records, sickness absence
- records, occupational health records, medical reports, pre-employment medical screening tests, insurance claims and
- information about criminal convictions and offences.

This special category data is processed in line with Art 9 (2)(h) of the GDPR, where it is necessary for the assessment of the working capacity of the employee and in the provision of or management of health or social care services.

We may receive and process information about you from:

- yourself (data you provide)
- ourselves (data we generate)
- your nominated referees & previous employers
- tax authorities
- pension providers
- medical professionals
- DBS

As an employee of Specialist Education Services Ltd, we process your personal data for the purposes of the performance of the contract of employment, including discharge of obligations laid down by law, management, planning and organisation of work, equality and diversity in the workplace, Health and Safety at work and for the purposes of the exercise and enjoyment of rights and benefits related to employment and for the purpose of the termination of the employment relationship.

We may transfer certain data to our payroll provider as necessary to make payments. We don't normally transfer your personal data outside the UK, however, should this be necessary, we will transfer your personal data using the appropriate lawful transfer mechanisms.

We pass certain data on to third parties including HMRC, your/our Bankers, Insurance Companies, the Disclosure and Barring Service and the Health and Safety Executive, local authorities and regulatory bodies such as Ofsted & CQC. We may receive and retain personal data about you from the Disclosure and Barring Service and your nominated Referees.

Our legal basis for holding and processing this information is our contract of employment with you, our public task in providing care and special education needs for our young people in our care, as well as to meet our legal obligations with regard to "Keeping Children Safe in Education" the "Care Standards Act", and "Children's Home Regulations 2015"

We may process photographic or video images of staff for the purposes of marketing collateral for our brochures, website and other printed publications where we may be displaying/celebrating evidence of our achievements, talents, milestones, or showcasing and publicising the work we do at SES. We only process this information with your explicit consent and for the for the purpose of publicity and marketing. We will not disclose any other personally identifiable information, such as name, contact details, location, etc. We will not retain this information for any longer than we have a purpose to do so.

As required by the law and statutory guidance with regard to "Keeping Children Safe in Education" we may retain records for up to 75 years to meet our obligation regarding Section 175 of the Education Act 2002.

We have a legal obligation to keep certain records related to your employment and may retain these records for 7 years from date of termination (for example under: The Finance Act 2008 or the Reporting of Injuries Diseases and Dangerous Occurrences Regulations 2013).
Other data may be kept for up to 15 years from termination of employment in case there are queries about your employment, unless you request that we delete the data beforehand.
Documentation containing personal data relating to our safeguarding obligations will be retained for a period of 75 years, in line with regulatory requirements.
Pension related details are also kept for 75 years.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

You have the qualified right to request: Access to and Porting of your data; Rectification or Erasure of the data; Restriction of processing or to Object to the processing.

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail.

You also have a right to lodge a complaint with a Supervisory Authority, for example the Information Commissioner's Office or http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

Our Data Protection Officer can be contacted at dpo@priviness.eu

Young Persons' Privacy Notice

What's this about?

The law that ensures that people keep your personal information safe – things like your date of birth, where you have lived, where you went to school. Specialist Education Services and other people collect and use information for all kinds of reasons, and the new law tells them exactly what they are allowed to do with yours.

We collect some information about you. It's our job to tell you how we will collect the information, how we will record it and how we will use it.

In this notice, you will see different names or terms used that you may not be familiar with, such as:

Data controller: This person or group of people, like Specialist Education Services is in charge of the information we collect.

Data processor: This person processes information for the data controller. This can be someone outside Specialist Education Services or Specialist Education Services itself

Data protection officer (DPO): This person makes sure we do everything the law says. Specialist Education Services' DPO is a company called Priviness.

Personal data: This means any information that can be used to identify someone, such as their name, email address and date of birth, or any information that relates to you.

Who looks after your information?

Specialist Education Services is the data controller of the personal information you give us – we look at how and why your information is collected and used. Our address is -

Specialist Educational Services Ltd
The Old Vicarage
School Lane
Heckingham
Norfolk
NR14 6QP

Sometimes we have to give your information to other people, such as the government, but we will only give away your information when you say it's ok *or* when the law or regulation says that we have to. When your data is given to someone else, they must look after it and keep it safe.

Why do we collect and use your information?

We will only collect your information when we need it to help us do our job or to follow the law. When we've collected it. Here's how we use it –

- To support your care and safeguarding
- To monitor and report on your progress
- To provide appropriate support
- To assess risk
- To assess the quality of our service
- To comply with the law regarding data sharing
- To inform and update the court or permitted organisations

What information do we collect?

The categories of information that Specialist Education Services collects, holds and shares include the following:

Your personal information
This is things like your name and date of birth.

Your characteristics
This means information about you, like where you're from, what language you speak and things like that.

Your care needs
This means information provided by your local authority about your care needs and risks.

Your attendance information
We will also record how many times you missed school or activity programme and the reasons why.

Your assessment information
We collect your assessment information and any test results when you sit a big test or exam or undertake a care assessment.

Some of your medical information
We keep information about any times you've been ill and any special conditions you have that we need to know about to keep you safe. We ask you to sign a consent form to give us access to your medical records or liaise with the Doctor on your behalf; this is to ensure your wellbeing and the wellbeing of others

Behavioural information
We record the number of times there have been behavioural issues, what the reasons were and any consequences.

Do you have to give us your information?

You must give us quite a lot of the information we need, but there is some information that you can choose whether to let us have it or not.

When we ask you for information that you don't have to give us, we will ask for your permission and let you know why we want it and what we will do with it. If you don't want us to have this information, that's your choice.

Are there some circumstances where I cannot have access to information about me?

There are certain circumstances where we can withhold information about you, for example where the information might cause serious harm to your physical or mental health or to another individual
There are also certain circumstances where we can withhold information about you, for example where there are safeguarding concerns about you or another individual.

How long will we keep your information?

We don't keep it forever, only as long as we need it to help us do the things, we need it for. We have a policy that tells us when to keep it and when to bin it.

Will your information be shared?

We won't share your information with anyone else without your permission, unless the law says we can or should. We may share information with:

- The Local Authority including educational establishments
- The NHS
- The Criminal Justice System- Court, Police, YOT and Probation
- Social Care Workers and Professionals
- Ofsted

The information that we share with them includes:

- Progress in care
- Any behavioural concerns
- Risk assessments
- Update information

Sometimes we have to share your information. We have a duty to share information with our regulatory bodies; this includes Ofsted, Care Quality Commission (CQC) and Regulation 44 visitor. They may ask us to share things like:

- How many young people in our care?
- Attendance figures
- Performance data
- Number of incidents of absconding
- Number of restraints
- Number of complaints
- Number of safeguarding concerns

The education information may be stored in the National Pupil Database, and then share some of it with people looking to help young people like you. But don't worry, the database is very safe, and your information won't get lost or given to anyone who shouldn't have it. We have to pass on certain information to the people in charge of local schools called the Local Authority. We might share some information with people who provide education and training for people over 16, like colleges. We may pass on information that helps them to make sure they provide the right kinds of education, such as your name, date of birth, where you're from and things like that.

We have to share some information with careers services once you reach 16.

What are your rights?

You have the right to:

- Be told how we use your information.
- Ask to see the information we hold.
- Ask us to change information you think is wrong.
- Ask us to only use your information in certain ways.

- Tell us you don't want your information to be processed. Unless we have a legal reason to do so.

If the information we are collecting is information that you can choose not to give, you can tell us to stop collecting it at any time.

If you're worried about how we get and use your information, you can speak to anyone at Specialist Education Services, who will be able to help you and answer any questions that you have.

If you want to speak to somebody not at Specialist Education Services, you can call the people who look after information, called the Information Commissioner's Office (ICO), on 0303 123 1113 or using their live chat.

Our Data Protection Officer can be contacted at dpo@priviness.eu

Four important things to understand

Now you've read this, we hope you understand that:

- The law allows us to collect and use your information to help us do our job.
- We may share your information with others, but only when we really need to.
- We will ask for your permission to share your information whenever you have a choice.
- You can tell us not to share your information, even when you have said yes before.

Would you like to know more?

If you have any questions, we will be happy to help you.

Changes to this notification

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail or delivered by hand.

APPENDIX C

Specialist Education Services Appropriate Policy Document

Guidance for Completion

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document demonstrates the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it outlines our retention policies with respect to this data. (See Schedule 1 Part 4).

You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However, if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

1. *(a) the condition which is relied upon;*
2. *(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and*
3. *(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.*

The APD therefore complements your general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge. See Schedule 1 Part 4 paragraph 40.

DESCRIPTION OF DATA PROCESSED

Purposes for processing

The following is a broad description of the purposes for processing of personal information:

- assessing an employee's fitness to work;
- complying with health and safety obligations;
- complying with the Equality Act 2010;
- complying with the Children's Homes (England) Regulations 2015, Care Standards Act 2000
- checking applicants' and employees' right to work in the UK;
- verifying that candidates are suitable for employment or continued employment; and
- to fulfil our safeguarding duties to the young people in our care.
- complainants, correspondents and enquirers
- advisors, consultants and other professional experts
- suppliers
- current and former employees, agents, temporary and casual workers, and volunteers
- CCTV recordings

Categories of Individuals

- young people in care
- employees
- recruitment candidates
- professional advisors
- care workers

Types of personal data we process

- personal details (such as name, address and biographical details)
- family, lifestyle and social circumstances
- education and training details
- racial or ethnic origin
- political opinions
- religious or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition, both declared and suspected
- sexual life
- gender
- offences (including alleged offences)
- criminal proceedings, outcomes and sentences
- physical identifiers
- representatives of individuals in this list, such as parents, other relatives, guardians, and people with power of attorney
- Custody and Biometric data (including Photographs)
- Contracts and Vetting of Staff and Officers
- Training and development records
- Employees, including staff, agency, contractors and volunteers
- Suppliers
  Complainants, enquirers and correspondents
- sound and visual images (CCTV)
- financial details
- licences or permits held (e.g driving licences),
- information relating to health and safety
- complaint, incident, and accident details
- opinions and assessments of care workers and staff

The types of personal data we process will vary depending on the purpose. We aim to process the minimum amount of personal data necessary for the relevant purpose.

SCHEDULE 1 CONDITION FOR PROCESSING

Specialist Education Services will process vast amounts of data for the purposes of:

- The care and safeguarding of young people
- Adherence to regulatory and statutory obligations

As a social service and care provider, we 'could' be relied upon, under Schedule 1 of the Data Protection Act to capture both operational and administrative / employment data as well as further sharing with partner agencies, local authorities and professionals.

Part 1 Processing: Conditions relating to employment, health and research etc

- Employment, social security and social protection
- Health or social care purposes

Part 2 Processing: Substantial public interest conditions

- Statutory etc and government purposes
- Equality of opportunity or treatment

Part 3 Processing: Additional conditions relating to criminal convictions etc

- Consent
- Protecting individual's vital interests
- Administration of accounts used in commission of offences involving children
- Extension of insurance conditions
- Processing by not-for-profit bodies
- Processing by regulatory bodies
- Legal claims
- Judicial acts
- Public health Research
- Support for individuals with a particular disability or medical condition
- Counselling
- Safeguarding of children and of individuals at risk
- Safeguarding of economic well-being of certain individuals
- Elected representatives responding to requests
- Disclosure to elected representatives

Privacy Notices: Please see appendices above (B) for further information.

PROCEDURES FOR ENSURING COMPLIANCE WITH THE PRINCIPLES

Accountability principle

Specialist Education Services detail all information in its Record of Processing Activities and multiple Privacy Notices.

All reasons, lawful basis, legislation and specifics of content shared are detailed in our data sharing agreements.

Specialist Education Services have appropriate Technical and Organisational Measure in place, including –

- Data Protection Policy
- Data Breach Procedure
- Data Erasure and Retention Policy
- Rights Management process
- Data Subject Access Request Procedure
- IT Security & Acceptable Use Policies

Data Protection Impact Assessments are carried out for uses of personal data that are likely to result in high risk to individuals' interests

Principle (a): lawfulness, fairness and transparency

Specialist Education Services have identified appropriate lawful basis for processing

Specialist Education Services details all information in its Record of Processing Activities and multiple Privacy Notices.

Information Notices are in place for Young People, Employees, Recruitment Candidates, Points of Contacts/Parents & Guardians, Suppliers & Professional Advisors.

All reasons, lawful basis, legislation and specifics of content shared are detailed in our data sharing agreements and Information Notices

Specialist Education Services are always open and honest in the collection and processing of personal data and do not deceive or mislead individuals regarding its use.

Principle (b): purpose limitation

Specialist Education Services have clearly identified our purpose(s) for processing the SC/CO data and the collecting and processing of SC/CO data is only processed for the intended purpose.

Specialist Education Services have included appropriate details of these purposes in our privacy information for individuals and are reflected in the Record of Processing Activities and Privacy Notices.

If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose or get specific consent for the new purpose, this decision is made based on consultation the DPO.

Principle (c): data minimisation

Specialist Education Services only collect SC/CO personal data we actually need for our specified purposes. This is revised and audited by our DPO annually. Any personal data that is no longer required will be deleted, anonymised or archived for statutory and regulatory requirements.

All data is held in line with retention schedule

There is a decommissioning process for legacy data which ensures old information is in the process of being deleted to ensure compliance

Annual weeding of paper files

Principle (d): accuracy

Specialist Education Services have appropriate processes in place to check the accuracy of the SC/CO data collected and record the source of that data.

Data is held in the Clearcare system and is checked and updated regularly and as required

Amendments are regularly made following a Rights of Rectification request, as alleged inaccuracies are flagged by the individual, which triggers an Information Management review.

Specialist Education Services do have processes in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we update it as necessary. This will be in line with the Retention Schedule

Specialist Education Services have policies and procedures which outline how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification and all other rights. Specialist Education Services have a Rights management Process & Policy in place.

Principle (e): storage limitation

Specialist Education Services carefully consider how long we keep the SC/CO data and are bound/guided by various regulatory and statutory obligations for the retention of data relating to children and young people in care. All data is held in line with retention schedule.

There is a decommissioning process for legacy data which ensures old information is in the process of being deleted to ensure compliance.

Specialist Education Services regularly review our information and erase or anonymise this SC/CO data when we no longer need it.

Specialist Education Services rely on the Retention Schedule and Asset Register. This covers both automated and manual deletion of data that is past its retention date.

There is a new Decommissioning Process that has been implemented post GDPR to assess and record all decisions to either archive or dispose of legacy data systems and or legacy data.

Principle (f): integrity and confidentiality (security)

Specialist Education Services have analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data.

Specialist Education Services have put appropriate technical measures in place for the safeguarding of Young people's sensitive personal data, including secure cloud storage, encryption and secure networks as described in the IT Security Policy.

The IT Security Policy is regularly reviewed and updated in line with requirements.

Both IT Security and the DPO are involved in new processing activities and new technologies being employed for all new projects, this ensures privacy by design and also all the necessary checks for information security, including PEN Testing and Dark Web Monitoring.

Specialist Education Services have a thorough breach reporting process for Information Management, Information Security and Information Technology to ensure all losses of physical assets and data are recorded and reviewed within the ICO time frames. This is done in conjunction with our DPO.

RETENTION AND ERASURE POLICIES

Specialist Education Services have a Record of Processing Activities spreadsheet which specify the relevant retention period for the particular purpose of processing and categories of data processed.

Specialist Education Services have in place a Retention and Erasure Policy.