SPECIALIST EDUCATION SERVICES

Data Protection Policy and Practice

Date created or revised: 0820
Date of next review: 0622

SES Avocet House Ltd (4926028), SES Turnstone House Ltd (7972485) and SES Kite Ltd (12634002) are subsidiary companies of Specialist Education Services Holdings Ltd (7970185)

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 Principal of the establishment). 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 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 it's 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.

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.

An illustration of the SES standard wording can be found in the appendices.

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 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;
- 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 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.

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 Subject Notifications

APPENDIX A

Organisational Technological Measures

SES SERVERS

Both Avocet House and Turnstone House have Apple Mac 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 sites, 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.

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.

The System Administrator (currently System Solutions) 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

Data Subject Notifications

Specialist Education Services Ltd standard wording
< . . . illustrative purposes only . . . > Specialist Education Services Ltd is the controller. Our contact details are: Specialist Education Services Ltd The Old Vicarage School Lane Heckingham Norfolk NR14 6QP For queries related to this notice please contact: • the Principal via office@specialisteducation.co.uk or • our Data Protection Officer at DPO@priviness.eu. *<The exhibitors at this event will receive your contact details as shown on this card and may contact you directly without notifying you further as this declaration constitutes your consent. >* <We may retain this data for up to 1 year.> If you consent to this use of your data we will retain a record of your consent. DECLARATION OF CONSENT *I agree to my data being processed as described above. Please tick* ☐ *Signature . . . . . .* *Date . . . . . .* You have the right to withdraw consent at any time by contacting us or our Data Protection Officer at the email address above. You have the qualified right to request: access to and port your data, rectification or erasure of the data, restriction of processing, to object to the processing. 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