SPECIALIST EDUCATION SERVICES

Acceptable Use of Technology Policy and Practice

Date created or revised: 0923
Date of next review: 0124

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

CONTENTS

D Technology Monitoring Form
E Young Person Technology Equipment Initial Setup Check
F Process to set up Young Person technology devices
G Young Person Technology Contract

1 INTRODUCTION

We live in an age where technology and means of learning and communication through the use of technology are developing at an ever-increasing rate. Today's children are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. The Internet connects computers and technology worldwide and is used by millions of people. It is an invaluable source of information and communication that should be available for use by adults and children.

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.

2 RATIONALE

This document describes Specialist Education Service's policy and practice with respect to the use of technology, including the online world, and the publishing of its own website. The document should be read in conjunction with the Curriculum Intent Policy Statement, Computing Policy and Practice document, Safeguarding and Child Protection Policy, Relationships and Sex Education Policy and Anti-Bullying Policy all of which outline specific issues underpinning the approach at each establishment. Reference to the framework 'Education for a Connected World 2020' will ensure children are supported to understand age specific advice about online knowledge and skills.

This policy and practice document relates to both children and adults.

3 GENERAL STATEMENT

We believe that the educational and social benefits of Internet access, online communication, learning and connecting through technology and the publishing of our own website far outweighs the possible risks involved, and that good planning and careful management will ensure appropriate and effective child use. Internet access is available to both children and staff and therefore this document refers to both.

Home Internet use has rapidly expanded, in parallel with the continued growth of mobile technologies, and has become an important part of learning and communication during education, work and leisure time. The Internet is managed by a worldwide collaboration of independent agencies that serve to attract a range of audiences and 'customers'. Without appropriate measures, access to unsuitable materials would be possible and security compromised. Equally by publishing our own website, access is possible for anybody in the world via the Internet. Therefore

appropriate measures must be employed to protect individuals in terms of privacy and exploitation.

4 THE IMPORTANCE OF THE INTERNET AND MOBILE TECHNOLOGIES

The purpose of internet access at SES is educational, social, cultural, leisure and managerial. Mobile technologies (3G/4G/5G) have expanded opportunities for both children and staff to access, interact and communicate educationally and socially using an increasing number of devices.

Access to the Internet is a necessary tool for staff and an entitlement for children who show a responsible and mature approach. It should be noted that the use of a computer system without permission or for a purpose not agreed by the establishment could constitute a criminal offence under the Computer Misuse Act 1990.

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in educational, social and cultural terms. These benefits include:

- Access to world-wide educational resources, e.g. museums and art galleries
- Information and cultural exchanges between children world-wide.
- News and current events.
- Cultural, social and leisure use in libraries, clubs and at home.
- Discussion with experts in many fields for children and staff.
- Staff professional development - access to educational materials and good curriculum practice, access to social work research and practice documents, access to up to the minute research in the health field.
- Communication with external advisory and support personnel, professional associations and colleagues.
- Exchange of administration data with outside bodies.
- Preparation for children for the world they live in.
- Entrepreneurial opportunities.

5 IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO CHILDREN

5.1 TEACHING ABOUT ONLINE SAFETY: UNDERPINNING KNOWLEDGE AND BEHAVIOURS

As the online word develops and changes at a great speed it is important to focus on the underpinning knowledge and behaviours that can help children to navigate the online world safely and confidently regardless of the device, platform or app. This teaching is built into existing lessons and learning opportunities across their personalised curriculum, covered within specific individual online safety lessons, Development and Learning planning, 24 hour learning, group sessions and focused interventions. Teaching and learning must always be age and developmentally appropriate, informed by the key adults specific knowledge of the young person as

well as the information provided by the 'Education for a Connected World 2020' framework.

Children will be encouraged to tell a member of staff immediately if they encounter any material that makes them feel uncomfortable. This includes situations of peer on peer abuse, cyberbullying or the sharing of nudes or semi nudes (see Sharing of Nudes and Semi-Nudes: advice for education settings working with children and young people and SES Safeguarding and Child Protection Policy and Practice Document).

The following knowledge and behaviours will be included:

5.1.1 How to evaluate what they see online

This will enable children to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. For example:

- Is this website/URL/email fake?
- How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?

5.1.2 How to Recognise Techniques Used for Persuasion

This will enable children to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity. SES can help children to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design).
- Criminal activities such as grooming.

5.1.3 Online Behaviour

This will enable children to understand what acceptable and unacceptable online behaviour look like. SES should teach children that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. SES should also teach children to recognise unacceptable behaviour in others. SES can help children to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline). to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online.
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

5.1.4 How to Identify Online Risks

This will enable children to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help children assess a situation, think through the consequences of acting in different ways and decide on the best course of action. SES can help children to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.
- Discussing when risk taking can be positive and negative,
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example.
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

5.1.5 How and When to Seek Support

This will enable children to understand safe ways in which to seek support if they are concerned or upset by something they have seen online. SES can help children by:

- Helping them to identify who trusted adults are (at SES this could be any adult whom they have built a trusting relationship, however, key adults will be their Case-Coordinator, Personal Tutor, Link Tutor, Learning Mentor).
- Looking at the different ways to access support from SES, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation (The SES Safeguarding and Child Protection policy and processes around reporting of safeguarding and child protection incidents and concerns to staff should be applied).

- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.
- Children will have specific sessions on cyberbullying and understand the procedures established within their establishment.

5.2 MANAGING THE RISK OF TECHNOLOGY AND INTERNET ACCESS

In common with other media such as magazines, books and video, some material available via technology and the Internet is unsuitable for children. SES will advise and support children and take all reasonable precautions to ensure that users access only appropriate material. There is also a comprehensive access and filtration system available through the safety management system, “Kerio”. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of inappropriate material will never appear on a technological device. Even with this policy fully implemented SES cannot accept liability for the material accessed, or any consequences thereof.

- Methods to quantify and minimise the risk will be reviewed formally, and remain under continual scrutiny in liaison with the ISP.
- SES will work with the Internet Service Provider and Safety Management System (currently Kerio) to ensure systems to protect children are regularly reviewed and improved, and meet the DfE filtering and monitoring standards.
- Children will be assigned an appropriate level on the Kerio E-Safety system (these are currently lead, bronze, silver and gold and the level of access for each can be found on the internal network).
- Staff will check that the sites selected for child use are appropriate to the age and maturity of children.
- Access levels will be reviewed as children’s Internet use expands and their ability to retrieve information develops.
- SES, its staff, parents, placing authorities and external advisers will work to establish agreement that every reasonable measure is being taken.
- The SES Principal will ensure that this policy is implemented effectively.
- The Registered Manager (LDPCP)will act as the lead professional for e-safety related concerns and issues.
- The senior management team will complete an annual audit of e-safety within the home and Learning Centre (see appendices).
- Each child will have an IT related section within their individual risk assessments and daily care.
- Regular checks will be established for all children incorporating all of their devices, at intervals appropriate to their individual needs (see section 5.7).
- All children will sign a technology contract drawn up by their key team of adults (see appendix G).
- All new devices issued to or owned by children will be set up/checked to ensure that age restrictions/permissions are in place where necessary (see section 5.6).
- New technologies are embraced as a potential learning opportunity but assessed for risk on an ongoing basis.
- Children will be informed of their responsibilities.
- Children will be informed that checks can be made on files held on the system.

- When copying materials from the Web, children will observe copyright.
- Children will be made aware that the writer of an E-mail or the author of a Web page may not be the person claimed.
- Children will be taught to expect a wider range of content, both in level and in audience, than is found in a library or on TV.

5.3 AUTHORISING ACCESS

- Internet access is an entitlement for children based on responsible use, and each young person will have a dedicated laptop.
- Parents will be informed that children will be provided with Internet access where it is important to support their learning, across the school day, the extended '24hr curriculum' and some social/leisure use.

5.4 MANAGING E - MAIL

- Children are expected to use E-mail as part of the National Curriculum and broader learning.
- All children will be provided with a standard SES email address.
- Children are permitted further web host email provided it is within the parameters of their individual IT/Technology risk assessment and they comply with the conditions of their Internet user agreement. This does include children agreeing to a systematic and proportionate level of monitoring and checking by adults.
- Communications with persons and organisations will be managed to ensure appropriate use and that the good name of SES is maintained.

5.5 SOCIAL NETWORKING FOR YOUNG PEOPLE

- Social networking sites are acceptable provided individual children can demonstrate responsible use within their individual IT/Technology risk assessment and they comply with the conditions of their Internet user agreement.
- Most social networking sites have age limitations; therefore children will only be eligible for consideration to join a social networking site, once they have reached the required age.

5.6 MANAGING OTHER FORMS OF MOBILE AND PERSONAL TECHNOLOGY

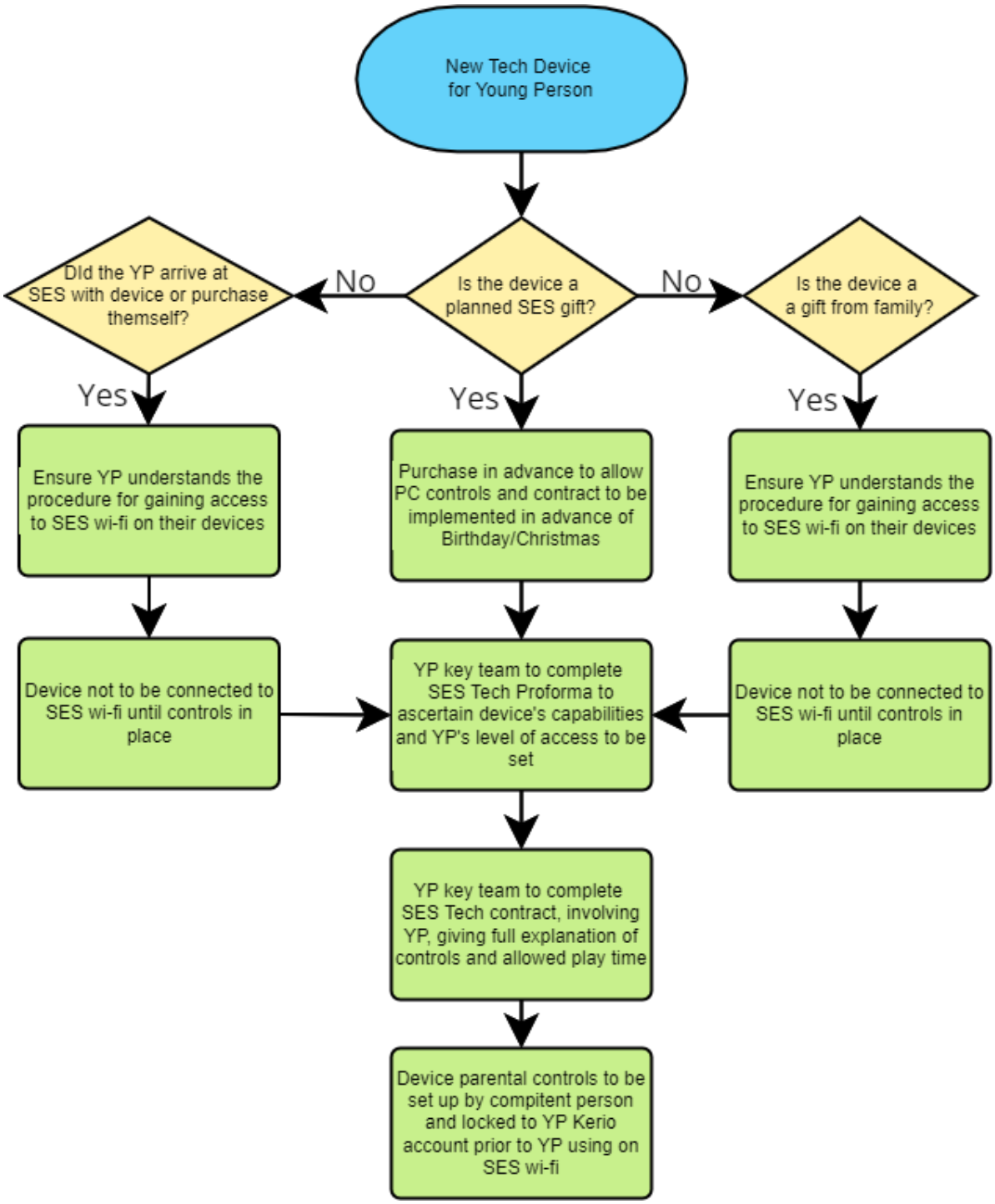
Children may be allowed consoles, mobile phones, tablets, and other handheld devices on a personalised basis; these decisions will be monitored through individual risk assessment and regular technology checks. This will also be supported by an individual technology contract (see appendix G).

Kerio, or any other internet filtering system, can only maintain security and safety for devices connected to the installed SES system; therefore devices that connect using mobile technology such as 3G/4G/5G need particularly stringent checks.

One of the primary issues with technology for young people at SES has been setting appropriate parental controls from the onset for new devices. It is essential this is completed in advance of the young person receiving the device as

retrospective settings often result in resistance and resentment from young people as it gives a feeling of being downgraded with the devices functions limited and restricted play time. Devices bought for Christmas or as birthday presents must be purchased in advance so careful thought is given to setting the device up correctly before the young person receives it. **Advice on how to do this is provided in appendices E and F).** This avoids the young person setting up the device themselves, which often results in an adult account being used that cannot be downgraded to work with parental controls. Advance planning also allows a technology contract to be instigated for the device (see appendix G

<u>Suggested SES Process for setting up new technology devices</u>



5.7 MONITORING SAFETY AND SECURITY

SES has a remote E-Safety monitoring system as well as the standard in house filtering and monitoring systems regarding appropriate use and safety**.** Additional monitoring processes are outlined below to support the managing of risk (see section 5.2):

- All children's machines will undergo regular monitoring to ensure appropriate internet use, at intervals appropriate to each child.
- Monitoring of social networking usage will be part of the regular monitoring process.
- The SES Principal will monitor the overall effectiveness of Internet access strategies. This will be achieved through a combination of a commercial remote monitoring system and in house systematic monitoring.
- Personal Tutors and Link Tutors will be trained in systematic checking of the children's computers and other items that have Internet capability or the provision to transfer information and/or pictures. These checks will be at the intervals set in the individual child's Daily Care. It is ultimately the Personal Tutor's responsibility to ensure the monitoring is carried out. These checks will be recorded on the Technology Monitoring Form (See Appendix D), stored in case files and on the SES network.
- A weekly Kerio alert will be sent to all Personal Tutors outlining all related Internet history for that week for their children.
- Monitoring may move to a more infrequent sample monitoring for individuals with an extended track record of responsible use.
- The senior management team and system administrator will ensure that regular checks are made on files to monitor compliance with this policy.

5.8 HANDLING COMPLAINTS AND INCIDENTS

- Responsibility for handling complaints and incidents will be given to the Head of Education and Registered Manager.
- Children and parents/carers will be informed of the procedure.
- Parents/carers and children will need to work in partnership with staff to resolve any issue.
- As with other issues, there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
- If staff or children discover unsuitable sites, the URL (address) and content will be reported to the Service Provider.
- Any material that staff suspect is illegal will be referred to the appropriate authorities via the system administrator.
- A range of consequences, including sanctions if necessary, may be imposed for inappropriate use, parents/carers may be informed and a child may have Internet or computer access denied for a period.
- Denial of access could include all work held on the system, including any examination work.

The SES Safeguarding and Child Protection Policy should be read when dealing with technology related incidents*.*

5.9 COMMUNICATION AND RESPONSIBLE USE

- Rules for Internet access and responsible use will be made clear to individuals and groups.
- All staff will have access to the Acceptable and Safe Use of Technology Policy, and its importance explained.
- Children, parents' and placing authorities' attention will be drawn to the Policy via the admission process.
- Periodic reminders and discussions about responsible Internet use will be included in the PSHEE (Personal, Social, Health and Economic Education) programme and Relationships and Sex Education curriculum covering both Learning Centre and home use.
- Staff will assist, where applicable, parents/carers to develop a well informed and balanced view of the risks and benefits.
- Joint home/school agreement on issues such as safe use of the Internet and other forms of electronic communication, will be established during the admission process.

5.10 CHILDREN'S INVOLVEMENT

There will be a bespoke technology access 'curriculum' programme for children that includes e-safety modules. This is intended to demonstrate responsibility in respect of access to and use of their own laptop. The 'curriculum' will include understanding of the benefits and drawbacks of Social Networking sites, and broader online safety. Effectively this will take place in the induction period for new admissions. Individual childrens personal equipment with Internet capability will be managed through the individual IT/Technologyrisk assessment process. Discussions about current and future use of technology will be part of monthly key worker meetings and the PAN process.

6 IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO ADULTS

Use of the Internet and technology by employees of Specialist Education Services is permitted and encouraged where such use supports the goals and objectives of the business.

However, Specialist Education Services has a policy for the use of the Internet and technology whereby employees must ensure that they:

- comply with current legislation;
- use the internet, technology and social media in an acceptable way;
- do not create unnecessary business risk to the company by their misuse of the internet, technology or social media.

All staff receive training on safe use of the Internet and technology as part of their safeguarding module in their induction period. All staff will receive annual e-safety online updates as part of training and professional development.

Safeguarding training supports adults to understand the breadth of issues classified within online safety, categorised into four areas of risk:

- Content - being exposed to illegal, inappropriate or harmful content; for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact - being subjected to harmful online interaction with other users; for example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your children, students or staff are at risk, please report it to the Anti-Phishing Working Group.

6.1 UNACCEPTABLE BEHAVIOUR

In particular the following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material;
- using the computer to perpetrate any form of fraud, or software, film or music piracy;
- using the internet to send offensive or harassing material to other users;
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- hacking into unauthorised areas;
- publishing defamatory and/or knowingly false material about Specialist Education Services, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format;
- revealing confidential information about Specialist Education Services in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of malicious software into the SES networks;
- using a personal hotspot (e.g. via a mobile phone 4g signal) to allow a young person access to online services.

6.2 COMPANY-OWNED INFORMATION HELD ON THIRD-PARTY WEBSITES

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of Specialist Education Services This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

6.3 ELECTRONIC COMMUNICATION BETWEEN STAFF AND CHILDREN

The SES Principal and/or Deputy Principal, Registered Manager or Head of Education must approve any proposed electronic communication with children.

This applies to many potential areas, and includes social networking, mobile phones, online gaming and personal email. Decisions will vary depending on whether the child currently resides at an SES establishment, or has left our care.

For children residing with SES:

- Staff should not provide their personal mobile phone number; any calls required to a child should be made using the 141 prefix to protect their details.
- Web based email addresses should not be shared between children and staff.
- There should be no direct connections on any form of social media or through chatrooms within online games between staff and children.

When a child/young person leaves an SES establishment staff should:

- Seek approval before making any form of electronic communication with a child or young person.
- Consider the age, maturity and appropriateness of the child/young person.
- Discuss the level of trust and responsibility that the information sharing places on the child/young person.
- Establish with senior managers the reasons for communication, and the type of information that can be shared.
- Maintain the highest level of professional standards, considering the reputation and confidentiality of young people and staff within SES.
- SES has no direct control over the communication received from young people that have left the establishment; therefore staff maintain contact at their own personal risk in line with safeguarding protocols and safer working practices.
- Any concerns should be reported to the SES Principal without delay.

6.4 SOCIAL NETWORKING SITES

Staff need to be aware of the dangers, boundaries and limitations in terms of how something said, either in person, or on line, may be interpreted by others. Social networking sites are no different than any other social setting and staff should be aware of how they represent themselves and the company in any form of conversation. This is a particularly sensitive issue when working with Looked After Children whose life chances and experiences for much of their formative years have effectively led them to be in our care. All staff have a professional duty that extends to passive receipt of comments and material that is derogatory of the children, colleagues or the company, as well as the writing of such.

6.5 MOBILE PHONES

All staff should have a mobile phone available whilst at work to maintain contact with the home or Learning Centre when engaging with children and young people on activities. However, the use of a mobile phone is potentially a sensitive issue; it can be both helpful and engaging as a learning tool, whilst also presenting as a clear rejection to a child. For example, if a child is with a staff member who diverts their attention to their phone, whether to take a call, receive or send a message or

simply to browse the internet, the child will potentially feel secondary to the device. This would be the same as ignoring a child or turning attention to another person. All staff must recognise the importance of role modelling socially acceptable behaviour in these situations.

Staff may request to receive emails or access work calendars on their personal phone; this is not an expectation of SES, and the most secure system is to utilise the MacBook provided.

When engaging in activities with children or young people, staff may wish to capture images on their phone. It is essential these are downloaded at the earliest opportunity to the SES Staff network, with the original images or video deleted from their device and any cloud backups. Contravention of this guidance could lead to the adult being subject to the company's disciplinary procedure

6.5.1 Staff Use of What's App

The use of What's App as a simple, quick and effective communication tool between colleagues is permitted. There are several advantages for staff in using What's App when working directly with children as it immediately indicates when a message has been read by a colleague, e.g., if supporting a young person in a remote location and assistance is sought. It also allows a quick and convenient way for teams to share ideas within groups. Groups may be set up by colleagues, e.g., a shift team; staff must allow access to a senior manager to any group for auditing purposes if requested.

In line with the previous guidelines for appropriate use of technology, staff must ensure the following additional parameters are followed at all times:

- *Communication must only be through group chat and not peer to peer;*
- *No photos can be shared via the app;*
- *Young people to be referred to by initials only;*
- *Only day to day communication is to be shared via What's App, such as requests for immediate assistance, instant updates to colleagues or an activity idea;*
- *What's App cannot replace or substitute current SES accepted communication routes, e.g., emails for questions around casework;*
- *It must not be used to report sickness or in any situation where a phone call is possible;*
- *What's App must never be used to source cover;*
- *It cannot be used as a planning tool as all formal planning should take place as a team during designated non-direct time;*
- *Use of What's App is not an SES expectation or compulsory.*

What's App must never be a substitute for the established communication professional routes within SES. It is extremely easy for a recipient to misinterpret electronic messages and without intention cause offence.

Inappropriate use of What's App has the potential to lead to formal company disciplinary procedures being instigated.

6.6 MONITORING

SES accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee morale and the reputation of the business.

In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume and use of Internet and network traffic, together with the Internet sites visited.

6.7 DATA PROTECTION RESPONSIBILITIES

Staff are responsible for adhering to the principles of the General Data Protection Regulation that are defined in the SES Data Protection Policy and Practice document. Staff must ensure they follow the guidance for processing both their own and others personal information, with reference to the SES Data Protection policy and Practice document section 6 (Staff Responsibilities). In particular:

- 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 personal information must 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.

Adhering to the procedures outlined in the ‘Maintaining Security’ section below is essential to reduce the potential risk of a data breach of personal data relating to the children or the adults.

All staff are made aware of the importance of following the guidelines for working from home, as set out in specific SES DPIAs and issued to staff periodically in line with policy review cycles.

6.8 SANCTIONS

Where it is believed that an employee has failed to comply with this policy, they will be subject to the company's disciplinary procedure. If an employee is found to have breached the policy, this will result in disciplinary action and possibly dismissal.

7 MAINTAINING SECURITY

SES has established a range of security measures to ensure that the organisation and individuals protect personal data adequately.

System and Password Management

- The system administrator (currently Osiris IT) will ensure that the system has the capacity to take increased traffic caused by Internet use.
- The whole system will be reviewed with regard to potential threats from Internet access.
- The SES Principal and system administrator in partnership with Osiris IToversee password management for all technology use within SES. Staff and children are issued with passwords for their laptop, network and Internet filtering that must be kept secure.
- Each member of staff will be required to update their user login password for their laptop at least three times a year (password will be a minimum of eight characters, featuring a lowercase, uppercase, number and special character).
- The Kerio and SES Server passwords will be changed by the system administrator at a minimum frequency of twice per year.
- Remote access to servers is available by request to senior staff; this will be authorised by the Operational Director or SES Principal and access will be via a VPN that requires both the staff member's Kerio and server passwords to be entered.

Email Accounts

- All staff will be provided with an Office 365 email. Communication between staff using @specialisteducation.co.uk emails is automatically an encrypted service.
- External emails will be sent encrypted unless the recipient requests an unencrypted version is sent; where this is agreed to the recipient must acknowledge receipt of the information.
- The Outlook app on Staff MacBooks is a mirror of the Outlook online email account. In some circumstances staff may require access to their online office 365 email using their unique password; for example, whilst their MacBook is being repaired or for senior staff working across multiple sites. Staff must follow the working from home guidance if granted this access and keep their personal and work emails separate.
- Senior colleagues, or in some circumstances, staff with accessibility needs, may wish to have access to emails on their phone or iPad. This will only be granted on an individual basis, expecting that the device has either face or touch recognition and that all working from home protocols are adhered to. The final decision lies with the SES Principal based on the level of risk involved.
- The Outlook calendar is used to share important diary dates between staff. Access to this is via their personal Macbook; use of personal portable devices (e.g. phones, iPads) will follow the same procedure as the process outlined in the above bullet point. There is no expectation that staff should use their own devices for email or calendars; the safest route is the MacBook provided by SES.

- The system administrator will suspend a staff email account if a MacBook (or other portable device) is temporarily or permanently lost, or if there are concerns regarding the security of the email account.
- Only the system administrator can add, edit or delete email accounts, using two factor authentication.
- Adults should be made aware that there are clear demarcations about what can and cannot be sent by email, even to placement authorities, social workers, etc which may breach child and data protection guidelines, e.g. personal data. When responding to requests for information staff members should always check with the Registered Manager or the SES Principal before sending anything. Staff need to be aware that regardless of our own protocols issues do and will vary between the different local authorities with which we work.

Safe Working Practices

- If an adult needs to leave their computer unattended as a temporary measure whilst working, the screen saver (display lock) should be activated.
- If data is to be transferred on any form of portable media, this must be first discussed with the data manager (SES Principal) and be fully encrypted.
- Staff should regularly back up data to their secure area of the SES network.
- Digital media of SES children should be stored on the SES network at the earliest opportunity and not kept on staff laptops or other forms of technological devices once transferred from the source device.
- All laptops issued by SES to staff and children will have encrypted hard drive back ups wherever possible.
- Staff may communicate between groups using Microsoft Teams or What's App; the use of other social media forums is not permitted for work purposes.

Video conferencing and calls

- Meetings may be conducted through virtual means such as Zoom or Teams. In these circumstances staff must maintain confidentiality and consider the environment in which they participate in the meeting. For example, the potential to be overheard in a public setting or even within a shared home must be considered.

Online Staff Information Systems

- Staff will be provided with access to online tracking systems for children (for example, Clearcare). Access should only be made via the authorised username and password, which should not be made available to any other person.
- ClearCare is an online software system that SES use to record specific information regarding children and young people. All staff will be provided with secure log in details for this that must not be shared with any other person.

The SES Data Protection Policy and Practice document should also be read in relation to maintaining security and organisational measures.

8 WEBSITE MANAGEMENT AND PUBLISHING

- The website shall reflect the ethos, ethics, values and standards of the establishment and promote a positive reputation.
- Written agreement will be acquired as part of the admission process from parents and/or placing authorities for any work from children to be published on a website.
- The SES Principal will ensure that there are structures, systems and key responsibilities in place that uphold and support high quality content that reflects the ethos and vision of SES.
- Any complaint received from parents or placing authorities regarding any article on the website will be immediately investigated and appropriate action taken, which may mean the article being removed.
- Children will be identified by their first names only.
- Home addresses and personal details of staff and children will not be included on the website. Correspondence will be directed to establishments land mail address or e-mail address.
- National legislation and copyright laws shall be respected.
- Software licences will be respected.
- Children will be taught to publish for a wide range of audiences.

9 SOURCES OF ADDITIONAL INFORMATION AND SUPPORT

- Education for a Connected world
- Teaching Online Safety in Schools 2017
- Sharing Nudes and Semi-Nudes: Advice for Education Settings December 2020
- Keeping Children Safe in Education – Annex D (Online Safety)

10 APPENDICES

A Acceptable Use of Technology Statement
B Rules for Responsible Technology Use by Children
C Annual E-Safety Audit Checklist
D Young Person Technology Monitoring Form
E Young Person New Technology Equipment Check
F Process to set up Young Person technology devices
G Young Person Technology Agreement

APPENDIX A

Acceptable Use of Technology Statement

Staff and children using the Internet must accept and comply with the following guidelines.

- All Internet activity should be appropriate to staff professional activity or the child's education and for appropriate leisure;
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the company ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As E-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden;
- Adults may make use of Internet access for personal use outside specified work times only in accordance with the guidance in this documentation.
- Web based email should not be accessed in working time or in the presence of children

SES reserves the right to examine or delete any files, software or downloads that may be held on its computers and network and to monitor any Internet use and/or sites visited by any individuals.

Use of phones, including those with cameras and Internet access, will be permitted provided the children stay within the boundaries of reasonable use and their individual contracts. To ensure safety they will be subject to the same systematic checks that occur for other Internet accessible equipment. If necessary access will be restricted through individual children's risk assessments.

The sending of and posting of photos is a facility that is now an inescapable part of everyday use of modern devices and social networking sites for most people. Clearly our children may be vulnerable in respect of their decision making. Procedures will be underpinned by a rigorous education of all children at SES establishments regarding the opportunities and risks in relation to following areas:

- SMART phones
- Use of Social Network sites
- You Tube.
- Sending and posting of photos and other information
- Emerging Technologies.

This education will take the form of group PHSE/RSE curriculum work and individual personalised programmes appropriate to each individual. The curriculum underpinning progress towards the ICT Competence Award will form the initial intensive personalised programme for all new admissions, supported by the completion of e-safety curriculum modules.

APPENDIX B

Rules for Responsible Technology Use by Children

Computers and technology are to help our learning and our access to information. These rules will keep you safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret; the network and all information on the network is private property;
- I will not access other people's files;
- I will use the computers for learning and leisure activities;
- I will adhere to my agreed individual code regarding internet and communication technology use, including daily care, risk assessments and signed contracts.
- I will only E-mail people or organisations an SES adult has approved;
- The messages I send will be polite and responsible;
- I will not give personal information e.g. my home address or telephone number for myself or others, or arrange to meet someone, unless my parent, carer or SES adult has given permission;
- I will not take pictures or share any personal details of my peers;
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other children and myself;
- I understand that designated adults may check my computer files and may monitor the Internet sites I visit.
- I understand that regular monitoring checks by adults extend to all devices that have access to the Internet and mobile communication, and that can transmit information and pictures.
- The downloading of games or software is not allowed without specific permission from an authorised adult
- The use of foul or abusive language, racist or sexist or any discriminatory language is totally unacceptable.
- The sharing of nudes and semi nudes is totally unacceptable and will be considered as a potential criminal act.

APPENDIX C

Annual E-Safety Audit Checklist

The responsible member of the Senior Leadership Team is:	
Has SES got an E-safety Policy that allies with Norfolk guidance?	**Y/N**
When was the policy last updated/reviewed?	
The school E-safety policy was agreed by directors on:	
How is the policy made available for staff?:	
How is the policy made available for parents/carers?:	
Has E-safety training been provided within the last year for both young people and staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y/N**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Y/N**
Are all children aware of the homes E-safety Rules?	**Y/N**
Are E-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all children?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the E-safety Rules?	**Y/N**
Are staff, children, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Is Internet access provided by an approved Internet service provider which complies with DfE requirements (e.g. Regional Broadband Consortium, NEN Network)?	**Y/N**
Have E-safety materials from CEOP been obtained?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
Where appropriate, have teaching and/or technical members of staff attended training on the school's filtering system?	**Y/N**

APPENDIX D

TECHNOLOGY MONITORING FORM

Please complete a separate record for each technological device or machine

Young Person:		**Device Checked:**			
Adult Completing Check:		**Signed:**		**Date of Monitoring:**	

Area Monitored	**Comments/Findings**	**Actions**
All Folders on Hard Drive, including Desktop		
Internet History and Cache (for all web browsers on device)		
Downloaded Files & Images		
Social Media - Facebook Snapchat Instagram, TIktok, (public posts and direct messages)		

Email Accounts (sent and received, Outlook and web based)		
Photos and videos		
Individual Apps		
Audio and Video Call History		
Text Message / Messenger Apps History		
Contacts		
Other		

APPENDIX E

Specialist Education Services

Young Person Technology Equipment Initial Setup Check

Name of Young Person:

Name of Device:

	Process	Action Completed
1	Ensure young person understands the timescales for set up of new devices	
2	Check device and complete pro forma checklist (below)	
3	Parental controls agreed by key team / family / social worker (if applicable)	
4	Technology agreement compiled from template and signed by young person	
5	Technology agreement approved by social worker / family if applicable	
6	Agreed parental controls applied to device	
7	Specifics of device and controls entered on to database	

Technology Pro Forma Checklist

	YES	**NO**	**N/A**
Does the device connect to wi-fi?			
Does the device have mobile data connectivity?			
Does the device have a web browser?			
Does the device have built in parental controls available?			
Is it possible to restrict age inappropriate content and apps?			
Does the web browser need to be blocked? *(Consider any history of misuse)*			
Does the camera need to be blocked? *(Consider any history of misuse)*			
Does the young person need parental controls in place on the device? (*Consider age of child and any history of accessing inappropriate content or misuse)*			
Does the young person need time restrictions in place?			
Should the young person be allowed to keep the device in their room over night?			
Does the young person have permission to use social media such as Facebook and Instagram and messaging apps? *(Consider any CP issues that could prevent this)*			

Is it appropriate to use young person's chronological age as a guideline for app downloads and usage?			
PEGI age rating needed for young person on parental controls *(taking in to account answer to previous question)*			
Agreed usage time and restricted time periods			
Weekdays (term time) usage time	xx hours		
Weekdays (term time) restricted times that device is blocked		to	
Weekends usage time	xx hours		
Weekends restricted times that device is blocked		to	
Details of any further actions needed:			

Date completed:

Review date:

APPENDIX F

Process To Set Up Young Person Technology Devices

- Key team to complete technology pro-forma (with support from tech advisor if required)
- Key team to complete technology contract with Young Person
- Device set up with parental controls by someone with detailed knowledge of device
    - Android phones/tablets – Screen Time Labs parental control app (annual subscription in place at Avocet)
    - Apple iPhones – iPhone 8 and above set up with apple Screen Time linked to an adult control account
    - Nintendo Switch – Nintendo parental control app linked to adult Nintendo account
    - Sony Playstation – Sony parental controls linked to SES Sony network account
    - Xbox – Microsoft parental controls linked to SES Microsoft network account
    - Windows PC - Microsoft parental controls linked to SES Microsoft network account
- Kerio
    - Set up secondary Young Person account for sole use with personal tech
    - Bind tech device MAC address to Young Person Kerio tech account
    - Set up time limits for Young Person
    - Set up traffic rules for Young Person to deny internet access for set times
- All device names, account login, password and MAC address to be logged in a database against each Young Person

Further consideration should be given to different key teams having personal opinions about time limits which can be perceived as unfairness by Young Person if they get a stricter key team compared to another Young Person having a more relaxed one. An SES guideline based on age but also individual needs would be useful as a rough guide for different teams. It is essential to have a consistent, joined up approach within SES that key teams can apply in order to ensure there is no disparity for Young Person. This could be achieved by delegating one person to maintain an overview of all Young Person's tech in a database detailing for each Young Person:

- Device name
- Device MAC address
- What parental controls are set on the device in terms of age limits and screen time
- The Kerio account device is locked to
- Kerio time limits set for internet access to SES wi-fi

A 'low and grow' approach could also be used with regards time limits whereby young people could start off with a low daily time limit with the view to being able to increase it if the key team are confident the Young Person is not becoming solely dependent on tech as their recreational outlet.

APPENDIX G

Specialist Education Services

Young Person Technology Agreement

Name of Young Person:

Name of Device/s:

I hereby agree to the following terms of use relating to the above-named device/s:

1. Parental controls will be put in place by adults to restrict non-appropriate apps and websites. Any attempt to remove the parental controls will be considered a breach of the agreement
   The device/s will be set to age xxx or PEGI rating xxx

2. Apps to be blocked - none, camera app, web browser app (*delete as applicable)*

3. The use of a VPN will be considered a breach of the agreement

4. The device/s will be checked regularly by personal or link tutor. Personal tutors will keep a record of any login details necessary to make full checks (this will include login details for social media or email accounts as well as the devices unlock codes)

5. Cameras will not be used inappropriately, such as taking indecent photos/videos or taking photos/videos of other young people/adults without their permission. Any occurrence of such incidents shall be considered a breach of agreement

6. Inappropriate use of any voice recorder applications such as recording adult conversations shall be considered a breach of agreement

7. Phones, tablets and other tech devices are not permitted in the Learning Centre at any time of the day or during any offsite Learning Centre activities without prior consent (this may be granted for some post 16 students). If the device is evident in the Learning Centre a decision will be made by HoE to impose appropriate consequence

8. The device/controller/leads will be handed in to an adult each night when requested
   Hand in time will be xx pm during the week and xx pm at weekends
   (delete if device can stay in young person's room overnight)

If I fail to comply with the above contract I understand I will lose the use of the device for a period of xx days

Young Person Signature _____

Personal Tutor Signature _____

Date _____