SPECIALIST EDUCATION SERVICES

Acceptable Use of Technology Policy and Practice

Date created or revised: 0317
Date of next review: 0318

*SES Avocet Ltd (4926028) and SES Turnstone Ltd (7972485)
are subsidiary companies of Specialist Education Services Holdings Ltd (7970185)*

CONTENTS

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. Emerging technologies present new opportunities for learning and new challenges in terms of appropriate use and safety. The Internet connects together 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.

2 RATIONALE

This document describes Specialist Education Service's policy and practice with respect to the use of technology, including the Internet and World Wide Web, and the publishing of its own website. The document should be read in conjunction with the General Curriculum Policy Statement, Computing Policy and Practice document, Safeguarding and Child Protection Policy, and Anti-Bullying Policy all of which outline specific issues underpinning the approach at each establishment. 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, communication, learning through technology and the publishing of our own website far outweighs the possible risks involved in both, 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 growth of mobile technologies, and has become an important part of learning and communication during 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

The purpose of Internet access at SES is educational, social, cultural, leisure and managerial.

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 ASSESSING THE RISK

In common with other media such as magazines, books and video, some material available via 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.
- The Company, its staff, parents, placing authorities and external advisers will work to establish agreement that every reasonable measure is being taken;
- The Principal will ensure that the policy is implemented effectively.
- The Registered Manager 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 school. (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.
- All children will sign a technology contract drawn up by their key team of adults.
- 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

- New technologies are embraced but assessed for risk on an ongoing basis

5.2 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.

5.3 MAINTAINING SECURITY

- The system administrator 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;
- Children should be made aware of the dangers of information of any kind about themselves, adults or SES being sent over the Internet;
- 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 protection guidelines. When responding to requests for information staff members should always check with the Registered Manager or the 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.
- The Principal and system administrator oversee 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.

5.4 ENSURING EFFECTIVE LEARNING

- On admission, all children will participate in a series of e-safety modules that explain the benefits, risks and expectations of technology use within their establishment.
- Curriculum planning will identify opportunities to enrich and extend learning activities via access to the Internet;
- Children will be given clear objectives for Internet use as part of learning sessions;
- Children will be supported in the use of relevant and suitable websites, although some open-ended research tasks may require responsible internet use of children;
- Children will be informed of their responsibilities;
- Children will be informed that checks can be made on files held on the system;
- Each child's care plan will have a section which describes individual differences in terms of access to the internet where these apply;
- 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.
- All portable and new technology will be embraced as a potential learning opportunity.

5.5 SUPPORTING CHILDREN IN ACCESSING THE INTERNET AND ELECTRONIC FORMS OF COMMUNICATION

- ICT teaching should be widened to incorporate Internet content issues, for instance the value and credibility of Web materials in relationship to other media;
- Children will be taught to validate information before accepting it as true, and to discriminate between fact and opinion;
- 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;
- Children will be encouraged to tell a member of staff immediately if they encounter any material that makes them feel uncomfortable.
- Children will be taught the SMART rules of the Internet, use of mobile phones and being online, published on the 'Thinkuknow' website.
- Children will have specific sessions on cyberbullying and understand the procedures established within their establishment.

5.6 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 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;
- The forwarding of chain letters will be banned;
- Social networking sites are acceptable provided individual children can demonstrate responsible use within their individual IT risk assessment and they comply with the conditions of their Internet user agreement.

5.7 MANAGING OTHER FORMS OF MOBILE TECHNOLOGY

- Children may be allowed mobile phones, tablets and other handheld devices on a personalised basis; these decisions will be monitored through individual risk assessment and regular technology checks.
- Kerio can only maintain security and safety for devices connected to the installed SES system; therefore devices that connect using mobile technology such as 3G and 4G need particularly stringent checks.
- Games machines and consoles including Sony PlayStation, Xbox, Nintendo DS, Sony PS Vita all have the potential for Internet connectivity. Therefore this will also be subject to regular monitoring checks.

5.8 ENSURING 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.

- 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).
- All children's machines will undergo regular monitoring to ensure appropriate internet use, at intervals appropriate to each child.
- Social Networking sites will be assessed for appropriateness on a site by site basis. Monitoring of social networking usage will be part of the regular monitoring process.
- Staff will check that the sites selected for child use are appropriate to the age and maturity of children;
- The 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 monthly checking of the children's computers and other items that have Internet capability or the provision to transfer information and/or pictures. It is ultimately the Personal Tutor's responsibility to ensure the monitoring is carried out. These checks will be recorded on the Technology Monitoring Record Sheets, stored in case files and on the SES network (See Appendices)
- 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.
- Access levels will be reviewed as children's Internet use expands and their ability to retrieve information develops;
- The senior management team and system administrator will ensure that regular checks are made on files to monitor compliance with the Internet Access Policy;

5.9 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.

5.10 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 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 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.

5.11 CHILDREN’S INVOLVEMENT

There will be a bespoke technology access ‘curriculum’ programme for children that includes e-safety modules alongside the completion of an SES ICT Competence Award. 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 risk assessment process.

6 <u>IMPLEMENTATION AND PRACTICE SPECIFICALLY IN RELATION TO ADULTS</u>

Use of the Internet by employees of Specialist Education Services Ltd 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 whereby employees must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet

All staff receive training on safe use of the Internet and technology as part of their safeguarding module in their induction period.

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

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 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 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 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 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.

6.6 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 <u>WEBSITE MANAGEMENT AND PUBLISHING</u>

- 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 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.

8 APPENDICES

A Acceptable Use of Technology Statement
B Rules for Responsible Technology Use by Children
C Annual E-Safety Audit Checklist
D Technology Monitoring Form

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 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 pupils 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.
- Youth Produce Imagery (sexting) is totally unacceptable 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 pupils 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 pupils?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the E-safety Rules?	**Y/N**
Are staff, pupils, 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**
Hard Disk, including Desktop		
Internet and History and Cache		
Cookies		
Downloaded Files		

Emails from/to Mac Mail		
Web Based Email		
Facebook (Social Media)		
Photobooth / Photo Images		
Individual Apps		
Other (Including Sample Monitoring)		