SENDSCOPE
Independent School

E Safety Policy

POLICY WRITTEN BY:	**SENDSCOPE Principal Natalie Walsh**
DATE POLICY PREPARED:	**March 2022**
DATE POLICY REVIEWED:	**October 2025**
DATE FOR NEXT REVIEW:	**October 2027**

E-SAFETY: RESPONSIBLE USE OF ICT POLICY

1. Introduction

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate Students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This policy also highlights the need to educate students about misinformation, disinformation, and conspiracy theories**,** acknowledging the complexity of online threats.

The school's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Anti-Bullying, Curriculum areas and Data Protection.

2. The need for E-Safety

End to End e-Safety

E-Safety depends on effective practice at several levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of Web filtering.

The e-Safety Policy relates to other policies including those for anti-bullying and for child protection/safeguarding. The school has an e-Safety Coordinator who reports directly to the SLT team on a regular basis and the Child Protection/Safeguarding officer and the E-Safety Governor when the need arises. Our e- Safety Policy has been written by the school, building on current advice published. It has been agreed by Senior Leadership and the E-Safety Governor.

3. Entitlement

Why Internet use is important

The Internet is an essential element in life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

The school Internet access is designed expressly for student use and includes filtering appropriate to the age of students.

Students are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

The school ensures that the use of Internet derived materials by staff and students complies with copyright law.

Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Whilst the Internet is always available on the school network, Students should be taught and shown the need for selective use of the Internet for appropriate use. There is a great scope for research and educational use of the Internet.

Information System Security

School ICT systems capacity and security are reviewed regularly, and any changes are noted by the Senior Leadership Team and Principals. The Governors with responsibility for E-Safety will be informed of any changes made to school ICT systems. Virus protection is provided through Mcafee and is updated regularly. School security is monitored through Securly and the use of an independent IT provider who monitors the schools filtering system.

Cyber Security Standards

SENDSCOPE is committed to maintaining robust cyber security measures to protect students, staff, and sensitive data. The school adheres to the Department for Education's Cyber Security Standards, ensuring that all digital systems are secure, monitored, and regularly updated. Access to school networks and devices is restricted to authorised users, with strong password protocols and multi-factor authentication where appropriate. Staff receive training on identifying and responding to cyber threats, including phishing, malware, and data breaches. All devices used for storing or transferring student information must be encrypted and comply with the school's Acceptable Use

Policy. Regular audits are conducted by the Senior Leadership Team to assess vulnerabilities and ensure compliance with data protection regulations, safeguarding the digital environment for all learners.

E-mail

Students only use approved e-mail accounts on the school system which are class based and not named.

Students are taught to immediately tell a teacher if they receive an offensive e-mail.

Students are taught that they must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. Staff have the responsibility for checking all emails sent by students.

The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the School Website are the school address, e-mail and telephone number. Staff or students' personal information will not be published. All staff and Governors who are included on the website and on social media platforms in 'Meet the SENDSCOPE Family' have given written consent for this to be published.

The Principals have overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing student's images and work

Photographs that include students are selected carefully and students' full names are not be used anywhere on the website in association with photographs.

Written permission from parents/guardians is obtained before photographs of students are published on the School website.

Student's work is published with the permission of the student.

Holding of student's images and information relating to the students

Information relating to students should not be held on staff's own computers or data handling devices (pen-drives) unless they are encrypted as outlined in the schools internal procedures, if external data handing devices are required to transport student data then a request form should be given to the principal.

Similarly, students' images should not be held on any device that is not owned by the school.

Social networking and personal publishing

The school blocks/filters access to social networking sites.

Newsgroups are blocked unless a specific use is approved.

Students are advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

The school works closely with the Local Authority, DfE and the Internet Service Provider to ensure systems to protect Students are reviewed and improved.

If staff or students discover an unsuitable site, it must be reported to the E-Safety Coordinator or Principals.

Senior staff and the independent IT consultants ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with a school phone where contact with Students is required.

Managing use of AI (Artificial Intelligence)

In recognition of the growing presence of AI technologies in education, SENDSCOPE is committed to ensuring their safe and ethical use within the school environment. AI tools, including generative platforms such as Co-Pilot, will only be used under staff supervision and for clearly defined educational purposes. Staff must assess the suitability, accuracy, and potential risks of AI-generated content, particularly in relation to misinformation, bias, and safeguarding concerns. Students will be taught to critically evaluate AI outputs and understand the limitations of these technologies. The school will follow DfE guidance on filtering and monitoring AI use, and ensure that any AI-integrated systems comply with data protection regulations and SEND-specific accessibility needs. All AI use must align with SENDSCOPE's safeguarding principles and be reviewed regularly by the E-Safety Coordinator and SLT. Students or staff are not permitted to use any other AI platforms other than Co-Pilot on the school network.

Protecting personal data.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Implementation

Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

The school keeps a record of all staff and students who are granted Internet access. The record will be kept up to date, for instance a member of staff may leave or a student's access be withdrawn.

Parents/Guardians are asked to sign and return a consent form.

Assessing risks

The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its

implementation is effective.

Handling e-safety complaints

The school holds and records any misuse of the school's network and evidence, and outcomes of breaches are recorded.

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to The Principals.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Students and parents/carers will be informed of the complaints procedure.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Introducing the e-safety policy to Students

E-safety rules are posted in all networked rooms and discussed with the students at the start of each year.

Students are taught e-safety both in ICT and PHSCE lessons.

Students are informed that network and Internet use will be monitored.

Staff and the E-Safety policy

All staff will be given access to the school e-Safety Policy and its importance explained. Staff are made aware that Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct are essential.

Enlisting parents/guardian's support

Parent/Guardian attention is drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school Web site.

5. The Learning Platform

The Learning Platform is not only for information to be shared but also as a learning resource for all users of the school, including Students, staff, parents/carers and Governors, and as such access will be granted to any member of the school.

The school learning platform is a means to fully include all students in the teaching and learning process.

6. Basic Skills

The Principals recognise the need to have a solid foundation of basic skills. The Basic Skills Agency defines Basic Skills as "The ability to read, write and speak in English and/or Welsh and use mathematics at a level necessary to function and progress at work and in society in general." For this reason, we encourage Students to read aloud where possible, spell using school spelling strategies they learn in English and use correct vocabulary when speaking, incorporating ICT words wherever possible. Students also focus on basic Math skills when learning to produce tables and graphs using ICT.

7. **Inclusion**

The Principals place a high emphasis on inclusion and the right of all students being able to access the curriculum no matter what their needs. The school recognises the need to allow students, parents and guardians to access information and provides this information in varying formats if at all possible, when requested or identified. The use of the school learning platform has been identified as a means of inclusion and will be used as such, to share information and educational resources.

8. **Safeguarding**

SENDSCOPE is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment. A safer setting starts with safe staff. The Principals and staff will review this policy in line with the School Development Plan.

Appendices:

Appendix 1: Rules for Responsible Internet Use for Students

Appendix 2: Acceptable Internet Use Statement for Staff

Appendix 3: E-Safety Audit

Appendix 4: Internet use - Possible teaching and learning activities

Appendix 1:

SENDSCOPE

Rules for Responsible Internet Use for Students

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

- I will not access other people's folders
- I will only use the computers for schoolwork and homework
- I will ask permission from a member of staff before using the Internet
- I will only e-mail people I know, or my teacher has approved
- The messages I send will be polite and responsible
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, guardian or teacher has given permission
- I will report any unpleasant material or messages sent to me. I understand my report will be confidential and would help protect other students and myself
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Student name: _____ Parent/Guardian signature: _____

Student signature: _____ Date: _____

The school accepts no responsibility for inappropriate use of the Internet outside school, even when children are researching a school-based subject.

Appendix 2:

ICT Acceptable Use Policy for Staff and Other Adults

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school. This organisation is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment. A safer setting starts with safe staff.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Use of Internet Services

Below defines what the schools' position is on acceptable, unacceptable and forbidden use of the Internet.

Acceptable

• Accessing business related web sites in relation to the user's job

• Accessing web sites (OTHER than those containing pornographic, offensive or obscene material) for non-business-related reasons during breaks, lunch hours, before or after the working day

• Accessing specific sites using your own log-in details (e.g. internet banking)

Unacceptable (misconduct)

• Spending any periods of the working day (excluding breaks and lunch hours) looking at nonbusiness related Internet sites

• Making your password available for other people to use the Internet service on your behalf

• Downloading any copyright material without the owner's permission

Forbidden (gross misconduct)

• Downloading software used for hacking or cracking passwords.

• Making repeated attempts to access web sites that, because of their inappropriate content, have been automatically blocked.

• Tying up Internet resources on non-business-related activity, to the detriment of genuine business Internet usage. This includes: -

- Leaving live internet feeds open to collect news or sports results;
- Downloading images, video or audio streams for non-business related purposes;
- Deliberately accessing sites containing pornographic, offensive or obscene material
- Downloading pornographic, offensive or obscene material
- Using someone else's personal user account and password to access the Internet
- Attempting to circumvent/avoid any security features
- Use of ICT equipment to access any VPN (Virtual Private Network) or Proxy Server services is strictly forbidden, as well as the use of Tor browsers or plugins to access the dark web

Use of Email Services

Acceptable

• Communication in connection with SENDSCOPE's business

• Occasional personal use during breaks, lunch hours, before or after the working day

• Management access to read employees/users' mailboxes where there is a legitimate need, authorised by the relevant member of SLT, to do so (e.g. if a person is absent and important email is expected.)

Unacceptable (misconduct)

• Using email for personal, non-business-related communication during the working day, outside of normal break time to the detriment of the service

• Customising emails such as using a non-corporate backgrounds, logos or signatures

• Forwarding chain emails

• Subscribing to non-business-related mailing lists

• Overuse of services for personal, non-business-related communication during breaks, lunch hours, before or after the working day to the detriment of the service

• Sending non-business-related email directly to large distribution groups

• Sending files with non-business-related attachments (e.g. compressed files, executable code, video streams, audio streams, or graphical images) to internal or external parties

Forbidden (gross misconduct)

• Sending messages or files through internal email, or via the external mail gateways that contain discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content

• Sending sensitive business material to unauthorised internal or external recipients

• Sending emails from another user account without the appropriate approval or permission.

Use of PCs and Servers

Below defines what the school's position is on acceptable, unacceptable and forbidden use of PCs

Acceptable

• Storing corporate data

• Loading text, images, video or audio streams in connection with normal business

• Storing limited amounts of personal data on your PC

Unacceptable (misconduct)

• Loading unauthorised or untested software, i.e. software not purchased through the formal purchasing process. This includes, for example, software downloaded from Internet web sites, whether freeware or commercially sold, unless permission has been given by the Principals.

Forbidden (gross misconduct)

• Loading files containing pornographic, offensive or obscene content, whether in text, image, video or audio format

• Storing personal material which is protected by copyright, such as pictures, music, video, games etc, that has NOT been purchased by the school

• Deliberate, reckless or negligent introduction of a virus into the network.

• Storing confidential or personal data or information on removable media without taking adequate protection or encryption.

User Accounts and Passwords

Acceptable

• Using your own, personally assigned user account to carry out your work at SENDSCOPE

• Using administrator accounts to carry out your daily tasks in response to specific activities assigned to you by your manager

• Access to user accounts without the owner's explicit permission where there is a legitimate business need.

Unacceptable (misconduct)

• Sharing a password associated with any user account assigned to you.

• Allowing other members of staff to use a session established using an account personally assigned to you.

Forbidden (gross misconduct)

• Resetting the password associated with a user account assigned to someone else, without the owner's express permission.

• Requesting the password for a user account personally assigned to another member of staff

• Using a user account that has been provided to another member of staff without correct permission

• Using a session established by another user under their own personal account

• Using a privileged user account to access data where there is no specific business reason to do so

I have read, understand and agree to abide by the SENDSCOPE Acceptable Internet Use Policy.

Signed: _____ Date: _____

Appendix 3:

E-Safety Audit This quick audit will help the senior leadership team (SLT) assess whether the basics of e-safety are in place. Schools will also design learning activities that are inherently safe and might include those detailed within Appendix 4.

The school has an e-Safety Policy that complies with LEA guidance.	
Date of latest update:	
The Policy was agreed by Governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
How is e-Safety training provided?	
All staff sign an Acceptable ICT Use Agreement on appointment.	
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	
Rules for Responsible Use have been set for students:	
These Rules are displayed in all rooms with computers	
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	
The school filtering policy has been approved by SLT	
An ICT security audit has been initiated by SLT, possibly using external expertise.	
School personal data is collected, stored and used according to the principles of the Data Protection Act.	
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT	

Appendix 4:

Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Students should be supervised. Students should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK
Using search engines to access information from a range of websites.	Parental consent should be sought. Students should be supervised. Students should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids Yahooligans - - CBBC Search Kidsclick
Exchanging information with other Students and asking questions of experts via email	Students should only use approved email accounts. Students should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	Liverpool web-mail School VLE Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing Students' work on school and other websites.	Student and parental consent should be sought prior to publication. Students' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Focus on Film
Publishing images including photographs of Students. Students should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum	Parental consent for publication of photographs should be sought. Photographs should not enable individual Students to be identified. File names should not refer to the student by name.	Making the News SuperClubs Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Students should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share Students' work.	Students should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum