South Molton Community Primary School

E-Safety Policy (encompassing internet access and acceptable use)

Note: The school has a separate Social Media Policy

Review Date: Jan 2025 at T&L committee
Date of next review: Feb 2027

Staff consulted:Rosie Charles-Jones

Rationale
It is the duty of the school to ensure that every child in its care is safe, and the same principles should apply to the virtual or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which is not age-appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology. We recognise that e-safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

The aim of this policy, for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Technologies
ICT in the 21st century is continually developing and has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Gaming sites
- Text and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as smartphones and tablets

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others. Risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Radicalisation, extremism online;
- Requests for personal information;
- Viewing ‘incitement’ sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

A summary of the school's safety responsibilities are outlined below. This list will assist in developing a co-ordinated and effective approach to managing e-safety issues:

• The school will appoint an e-Safety Coordinator who may also be the Designated Child Protection Coordinator as the roles overlap, but could also be a member of SMT, the ICT Coordinator or a subject teacher. The e-safety Coordinator will receive support and advice from county advice, and where necessary, the Police.

• The e-Safety coordinator should maintain the e-Safety Policy, manage e-Safety training and keep abreast of local and national e-safety awareness campaigns.

• The school will review the policy every 2 years to ensure that it is current and considers any emerging technologies.

• The school will audit its filtering systems regularly using SWgFL to ensure that inappropriate websites are blocked.

• To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.

• The school will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem. This includes whole assemblies inline with e-safety week.

• All staff, governors & visitors must read and sign the Acceptable Use Policy.

• Parents should sign and return the e-Safety Rules consent form.

• The e-Safety Policy will be made available to all staff, governors, parents and visitors through the website.

Implementation and Compliance
No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

Why is Internet use important?
Developing effective practice in Internet use for teaching and learning is essential. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. The Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century 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. Pupils may use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating Internet Content
In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: clicking the e-safety icon, closing the page and reporting the incident immediately to the teacher. The school will

ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Local Area Network security

• Users must act reasonably;

• Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for dismissal;

• Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders; • Servers will be located securely and physical access restricted;

• The server operating system will be secured and kept up to date;

• Virus protection for the whole network will be installed and current;

• Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security

All Internet connections must be arranged via SWFL to ensure compliance with the security policy. Firewalls and switches are configured to prevent unauthorised access between schools.

• The security of the school information systems will be reviewed regularly;

• Virus protection will be updated regularly;

• Security strategies will be discussed with the LA when necessary;

• Personal data sent over the Internet should be encrypted or otherwise secured;

• Portable media may not used without specific permission followed by a virus check;

• Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail;

• Files held on the school's network will be regularly checked;

• The network manager will review system capacity regularly.

Emails

• Pupils may only use approved e-mail accounts;

• Pupils must immediately tell a teacher if they receive offensive e-mail;

• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;

• Whole-class or group e-mail addresses should be used in primary schools.

School Website

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images
Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published.

School video conferencing equipment should not be taken off school premises without permission because use over the non-educational network cannot be monitored or controlled. At present no video conferencing facilities exist in school. Users Unique login and password details for the educational video conferencing services should only be issued to members of staff and kept secure. Pupils should ask permission from the supervising teacher before making or answering a video conference call. Videoconferencing should be supervised appropriately for the pupils' age. Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.

Mobile phones are not to be brought to school by pupils and will be confiscated if found. Staff mobile phones will not be used or on display during school hours in any areas of the school where children are present. Only school registered cameras are to be used in school and no photos or videos are to be taken using mobile phones.

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

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

Internet Access

• The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications;

• All staff must read and sign the 'ICT Acceptable use policy' before using any school ICT resource;

• At Key Stage 1 and 2, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials;

• Parents will be asked to sign and return a consent form for pupil access.

Internet Risks
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the Council can accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

Passwords
- Use a strong password
- Do not write passwords down
- Passwords should not be shared with other children or staff.

E-safety Complaints

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

• All children will be taught to use the internet safely and to monitor and report abuse;

• Any complaint about staff misuse must be referred to the Head Teacher, unless it is the Head Teacher where complaints will be sent to the Chair of Governors;

• Parents and pupils will need to work in partnership with staff to resolve issues.

Introducing the Policy

• Safety rules will be posted in rooms with Internet access;

• Pupils will be informed that network and Internet use will be monitored;

• Instruction in responsible and safe use should precede Internet access;

• An e-safety module will be included in the Computing, Citizenship or PSHE curriculums covering both school and home use;

• All staff will be given the School e-Safety Policy and its application and importance explained;

• Staff should be aware that Internet traffic can be monitored and traced to the individual user; • Discretion and professional conduct is essential;

• Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;

• Parents' attention will be drawn to the school's e-Safety Policy in newsletters and on the website • Internet issues will be handled sensitively, and parents will be advised accordingly.

Websites offering additional advice and guidance

BBC Chat Guide http://www.bbc.co.uk/chatguide/ Becta http://www.becta.org.uk/schools/esafety
Childline http://www.childline.org.uk/
Child Exploitation & Online Protection Centre http://www.ceop.gov.uk
Grid Club and the Cyber Cafe http://www.gridclub.com
Internet Watch Foundation http://www.iwf.org.uk/
Internet Safety Zone http://www.internetsafetyzone.com/
Kidsmart http://www.kidsmart.org.uk/
NCH – The Children's Charity http://www.nch.org.uk/information/index.php?i=209
NSPCC http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Stop Text Bully www.stoptextbully.com
Think U Know website http://www.thinkuknow.co.uk/
Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com

Appendices

1. ICT Acceptable Use Policy for Pupils.
2. ICT Acceptable Use Policy for Staff, Governors and Visitors
3. E-safety Record of Concern
4. E-safety Record of Action

Appendix 1:

South Molton Community Primary School
ICT Acceptable use policy for pupils.

<u>This is how we stay safe when we use computers:</u>

I will ask a teacher or suitable adult if I want to use the computers.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

The messages that I send will be polite and sensible.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (parent): ……..

Appendix 2:

South Molton Community Primary School
ICT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anybody else.
- When accessing school emails or any other sensitive information relating to the school, employees will ensure that it is conducted on a device that has the appropriate security measures (anti-virus, firewall, encryption) and that it is locked out when away from the device and logged off each of the sites after use.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure that any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Headteacher.
- If it is necessary to bring my own personal devices to school, these will only be used during non-contact time without pupils.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will report any e-safety concerns to the designated e-safety safeguarding officer immediately using the e-safety Record of Concern.
- Mobile phones will be out of sight and switched to silent.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police. I understand the procedures and agree to follow them with immediate effect.

Print name: _____

Signed: _____ Date: _____

Appendix 3:

E-safety Record of Concern

<table>
<tr><td>Name of child</td><td colspan="2"></td></tr>
<tr><td>Child's DOB</td><td colspan="2"></td></tr>
<tr><td>Name of person completing this form</td><td colspan="2"></td></tr>
<tr><td>Date and time of incident/disclosure</td><td colspan="2"></td></tr>
<tr><td>Names of any other staff/children present</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Record any disclosure from the child using their words.
To clarify/gather information, use:
● Tell
● Explain
● Describe
● Outline

USE NO FURTHER QUESTIONS.</td><td>Who?</td><td>What?</td></tr>
<tr><td>Where?</td><td>When?</td></tr>
<tr><td>Why are you concerned about the child?</td><td colspan="2"></td></tr>
<tr><td>Detail anything you have observed and when</td><td colspan="2"></td></tr>
<tr><td>Detail any games/websites/films the child discussed with you. Include Avatar names, online friends' names and where known.</td><td colspan="2"></td></tr>
</table>

What category does the disclosure best fit with?	Grooming	
	Cyber-bullying	
	Misuse of social networking site	
	Sexting	
	Gaming	
	Underage films	
	Misuse of digital camera	
	Other (please specify)	
Detail anything you have heard and when		
Detail anything you have been told, by who and when		
Name (print)		
Date		
Position		
Signature		

Appendix 4:

E-Safety Record of Action

Name of e-safety co-ordinator/DSP record of concern handed to	
Date	
Summary of the recorded concern	
Action(s) to be taken	
Outcomes of action(s)	
Name	
Signed	
Date	