SUMMERHILL INFANT SCHOOL

Inspiring, nurturing and supporting each child, every day to develop citizens for the future. Our School lays the foundation for a lifetime love of learning

E-SAFETY POLICY

Document Summary

Document Owner:	Headteacher
Version:	4.0
Document Status:	Approved
Date Last Approved:	January 2025
Date of Next Review:	January 2026
Review Frequency:	Yearly
Governing Reviewing Committee/Governor:	SC&P
DfE Statutory or Optional policy:	O
Appendices:	None
On School Website?	No

Amendment History

Version	Amendment Date	Pg Num	Amendment Summary
2.0	Nov 2022	1 4	Inclusion of link to Equalities Policy No use of phones in classrooms except for medical reason
3.0	Nov2023	2-3	Section 4 – 2 additional information bullet points about filtering safety procedures.

Our e-safety policy has been written by the school, building on the Bristol e-safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

This policy has regard for the Safeguarding duty placed on Summerhill Infant School to protect the safety and mental and physical well-being of all pupils and Staff and should be read in line with our Equalities Policy.

The breadth of issues classified within online safety is considerable and ever evolving, but can be 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: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

1 Why is internet use important?

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.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, wellbeing and to support the professional work of staff and to enhance the school's management information and business administration systems.

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

2 How will internet use enhance learning?

The school's internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.

Pupils will learn appropriate internet use and be given clear objectives for internet use.

· Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

· Pupils will begin to be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation through termly e-safety lessons, progressing from Rec to Yr2.

· Useful E-safety websites to support Parents/Carers are on the School's website.

3 How will internet access be authorised?

All staff will automatically be granted internet access in school. Only school staff can access the internet in school. This includes temporary members of staff and authorised personnel who have sought permission.

Pupils' Parental Consent Form will include the acceptable use policy and guidance for video, sound and images for web publication.

For pupils, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

4 How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content.

· Staff will check that web content is appropriate before introducing it to children. If staff, parents/carers or pupils do discover unsuitable sites, the URL (address) and content will be reported to the internet Service Provider 0117 9037999 cyps.it.helpdesk@bristol.gov.uk

- BCC web filtering regularly reports use of inappropriate sites and key words to Headteacher to further investigate flagging up potential risks, this includes all devices connected to the school domain.
- All new websites visited are pre-screened/filtered by BCC before being made available for Staff and pupils. This and the above point address the changes made in KCSiE

· Computing Co-ordinator's will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school will work in partnership with parents, Bristol County Council, DCFS and the SWGfL to ensure systems to protect pupils are reviewed and improved.

5 How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school and Bristol Council will take all reasonable precautions to ensure that pupils 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. Neither the school nor Bristol County Council can accept liability for the material accessed, or any

SUMMERHILL INFANT SCHOOL

Inspiring, nurturing and supporting each child, every day to develop citizens for the future. Our School lays the foundation for a lifetime love of learning

consequences of internet access. All Staff have received PREVENT training and understand that extremist views can be found on the internet.

· The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

· The Headteacher will ensure that the internet policy is implemented and compliance with the policy monitored.

6 Managing Content

6.1 How will pupils learn to evaluate internet content?

The School will endeavour to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Specific lessons will be included within the Computing Scheme of Work that teaches pupils how to read for information from web resources.

The school will participate in an annual 'Internet Safety Day'

The headteacher will be responsible for permitting and denying additional websites as requested by colleagues.

· Training will be available to staff in the evaluation of web materials and methods of developing students' critical attitudes if required.

6.2 How should website content be managed?

The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

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 photographs of pupils are published on the school website.

Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified.

· The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

· The website will comply with the school's guidelines for publications.

· The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7. Communication

7.1 Managing e-mail

Pupils will only e-mail in school as part of the class. Whole-class or group e-mail addresses will be used. However:

· Pupil's will be taught that they must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

· Pupil's will be taught that if they receive abusive e-mails or are concerned about received messages they must tell an adult.

7.2 On-line communications

Students/pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety.

The school will conduct regular pupil views about home use of Computing. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.

7.3 Mobile technologies

· Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

· Mobile phones are not permitted for pupils within the school.

· Staff will not use personal mobile phones in the classrooms/ communal spaces with the exception of medical exemptions ie blood analysis etc

8. Introducing the Policy to Pupils

Rules for internet access will be posted in all rooms where computers are used.

A module on responsible internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal

information safe, how to use mobile technologies appropriately and using online communication appropriately.

· Instruction on responsible and safe use must precede internet access.

· Pupils will be informed that internet use will be monitored.

9. Parents/Carers and E-Safety

Parents/Carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Website.

Regular information will be provided to parents/carers about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.

· Internet issues will be handled sensitively to inform parents/carers without undue alarm.

· A partnership approach with parents/carers will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.

· Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents/carers.

· Advice about E-safety will be on the School's website, including links to support children at home eg 'You think you know.com'.

· Interested parents/carers will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).

· All parents/carers will receive support information as and when available, e.g. Know It All for Parents.

10. Consulting with Staff and their inclusion in the E-safety Policy

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained. It should be read in conjunction with the Social Media Policy and KCSiE guidance.

All staff must accept the terms of the 'Responsible internet Use' statement before using any internet resource in school.

Discretion and professional conduct is essential.

Only staff working in school will have access to the internet in school and any temporary members of staff will been given copies of the e-safety policy.

· Staff development in safe and responsible internet use and on the school internet policy will be provided as required.

11. How will complaints be handled?

Irresponsible use of the internet by pupils will be dealt with by class teachers in the first instance then referred to the headteacher and parents informed.

Any complaint about staff misuse must be referred to the headteacher.

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

· Parents/carers and pupils will need to work in partnership with staff to resolve issues.

· As with drugs issues, there may be occasions when the police must be contacted