

Bishopton Primary School



E-Safety Policy

Prepared by:	Andrew Smith
Ratified:	October 2023
Reviewed:	Emma Jones
Reviewed:	
Reviewed:	

Bishopton Primary School



Policy for E-Safety (also refer to the Computing and ICT Policy)

Introduction:

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Bishopton Primary School's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Habits:

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 from the Warwickshire Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

E-Safety co-ordinator:

The appointed e-Safety co-ordinators will be the Headteacher and the ICT manager.

Why is Internet Use Important?

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 information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will 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 refers to:

- The National Curriculum:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go to for help and support when they have concerns about content or contact on the internet or other online technologies



Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

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

Authorised Internet Access:

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- Parents will be informed that pupils will be provided with supervised Internet access.



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

World Wide Web:

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email:

- Pupils may only use approved e-mail accounts on the school system.
- 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 school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking:

- The LA will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering:

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing:

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.



Published Content and the School Web Site:

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Twitter, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Twitter.
- Work can only be published with the permission of the pupil and parents.

Information System Security:

- School ICT system's capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Assessing Risks:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Warwickshire City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Online bullying will not be tolerated in our school. Any evidence to suggest that this is taking place will be dealt with swiftly and decisively by the Headteacher in the same way that any bullying issues are dealt with (see anti-bullying policy).
- We will work with children to make them aware of the benefits and pitfalls of using the Internet and how to use it safely through workshops and specific assemblies. This will also be discussed during computing lessons as and when appropriate.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents will be informed of the complaints procedure. This will follow the guidance set out in the complaints policy.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.



Communication of Policy:

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff:

- All staff will be given the School e-Safety Policy and its importance explained (this will be regularly updated and reinforced).
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The online Safety leads will provide advice/guidance and training to individuals as required.

Parents:

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure, the school Website and Safer Internet Days.

This policy will be reviewed at any time on a request from the Governors, or at least once every three years.

Signed:

Date:



Referral Process – Appendix A

KS1 & KS2 Pupils Acceptable Use – Appendix B

E-Safety Rules – Appendix C

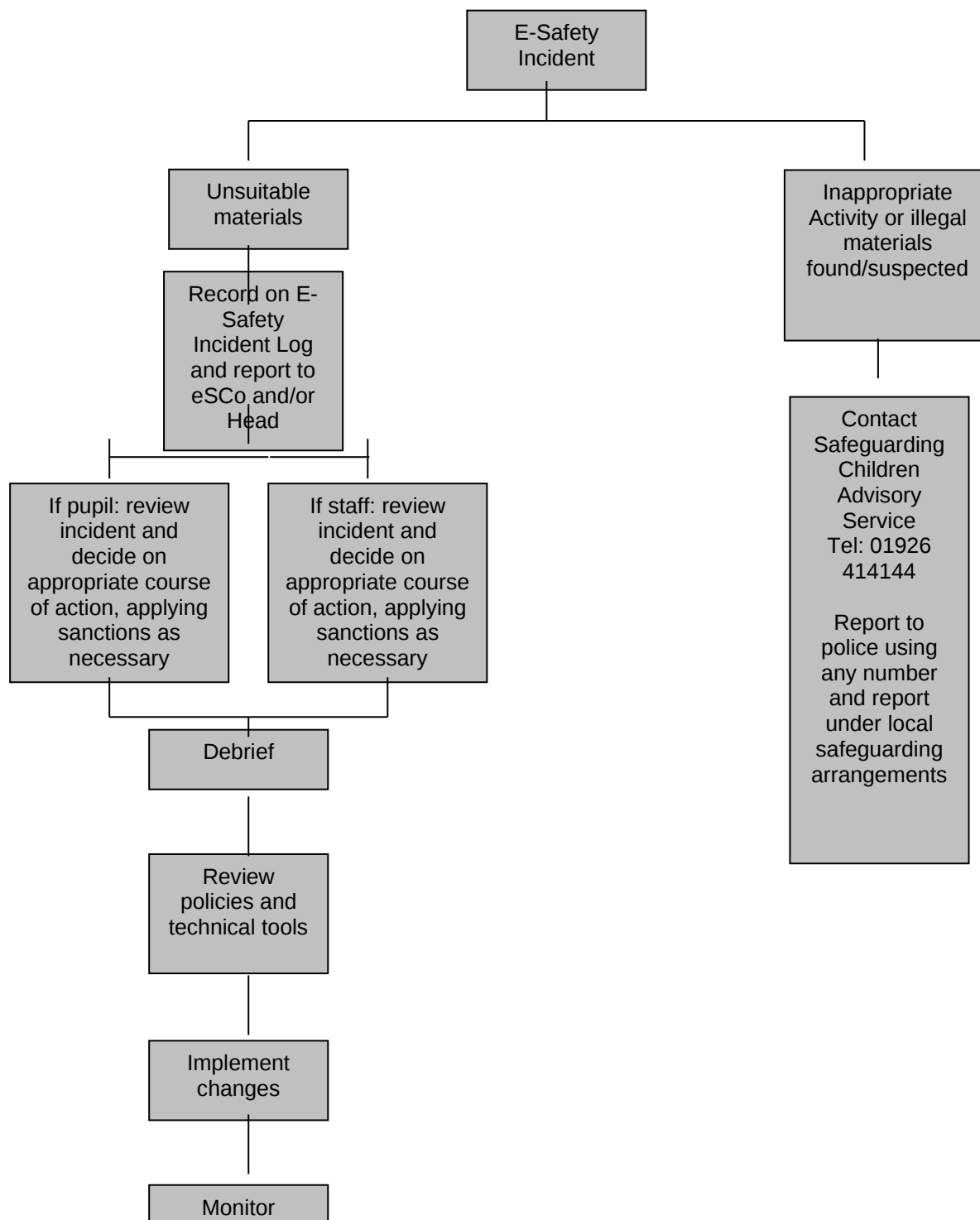
Staff Acceptable Use – Appendix D

School E-Safety Incident Log – Appendix E



Appendix A

Flowchart for responding to e-safety incidents in school



Adapted from Becta



Appendix B

Key Stage 1:

Think then Click	
These rules help us to stay safe on the Internet	
	We only use the internet when an adult is with us
	We can click on the buttons or links when we know what they do. 
	We can search the Internet with an adult.
	We always ask if we get lost on the Internet. 
	We can send and open emails together.
	We can write polite and friendly emails to people that we know. 

Key Stage 2:

Think then Click
e-Safety Rules for Key Stage 2
• We ask permission before using the internet. • We only use websites that an adult has chosen. • We tell an adult if we see anything we are uncomfortable with. • We immediately close any webpage we not sure about and think carefully before clicking on any links/adverts. • We only e-mail people an adult has approved. • We send e-mails that are polite and friendly. • We never give out personal information or passwords (Remember information can also be seen in photos and videos.) • We never arrange to meet anyone we do not know. • We do not open e-mails sent by anyone we do not know. • We do not use Internet chat rooms. • We are kind and respectful to others.

Appendix C

E-Safety Rules:

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.



Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Safeguarding Team.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: Capitals: Date:

Accepted for school: Capitals: ...



BISHOPTON PRIMARY SCHOOL E-SAFETY INCIDENT LOG

Date & Time	Initials of pupil or staff member & class	Laptop/iPad number	Details of incident (including evidence)	Actions and Reasons

