



E-Safety Policy

Date of Policy: Spring 2025

Review Date: Spring 2026

1. Who will write and review the policy?

- Our E-Safety Policy has been written by the Head Teacher building on the Bucks CC E-Safety Policy and government guidance. It has been agreed by the Senior Management, staff and approved by the Governing Body.
- The E-Safety Policy is part of the Computing Policy and relates to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship.
- The E-Safety Policy and its implementation will be reviewed annually.

2 Teaching and learning

2.1 Why is Internet use important?

The National Curriculum in England (2013) states that: pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

The national curriculum for computing aims to ensure that all pupils are responsible, competent, confident and creative users of information and communication technology.

- 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.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The Early Years Foundation Stage approach computing and internet use through their curriculum area of Understanding the world, which looks a development of the use of technology

2.2 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;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 Bucks CC and the DfE;
- access to learning wherever and whenever convenient.

2.3 How can Internet use enhance learning?

Developing effective and safe practice in Internet use for teaching and learning is essential. Teachers can help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

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

2.4 How will pupils learn how to evaluate Internet/World Wide Web content?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff

and pupils complies with copyright law.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3. Managing Information Systems

3.1 How will information systems security be maintained?

It is important to review the security of the school computer system. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Bucks CC advisers and Turn It On.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be 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 Computing Lead and the Schools IT provider will review system capacity regularly.

3.2 How will e-mail be managed

E-mail is an essential means of communication for both staff. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created.

In the school context, e-mail should not be considered private and the school reserve the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

In school:

- Access in school to external personal e-mail accounts will not be allowed.
- 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.

3.3 How will published content be managed?

The following protocol will be followed:

- The contact details on the website is the school address, e-mail and telephone number. Staff or pupils' personal information will 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 will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

3.4 Can pupil's images or work be published?

The following protocol will be followed:

- Images that include pupils will be selected carefully and only images of children with parental consent will be used.
- 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.
- Work will only be published with the permission of the pupil and parents.

3.5 How will social networking and personal publishing be managed?

Parents and teachers need to be aware that the World Wide Web has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: TikTok, wikis, Whatsapp, Facebook, Bebo, Piczo, Windows Live Spaces, Instagram, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The school will block access to social networking sites from children's' accounts.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location eg. School uniform, house number, street name or school.
- Teachers' official blogs or wikis will be password protected and run from the school website. Teachers will not run social network spaces for pupil use on a personal basis.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals.
- Pupils will be advised not to publish specific and detailed private thoughts.
- The schools is aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.

3.6 How will filtering be managed?

- All Internet access will be supervised. Internet access must be appropriate for all members of the school community.
- The school will work with Bucks Learning Trust and Turn It On to ensure that systems to protect pupils are regularly reviewed.
- Our filters are managed by Turn It on and comply with Bucks policy.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Computing Coordinator.
- Regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported.
- The school's filtering strategy is designed by educators to suit the age and curriculum requirements of the pupils, advised by Bucks GfL, Bucks Learning Trust and Turn It On.

3.7 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia

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 or whenever a child is in the vicinity. The sending of abusive or inappropriate text messages is forbidden.

3.8 How should personal data be protected?

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

4 Policy Decisions

4.1 How will Internet access be authorised?

- 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 'Internet Code of Conduct' before access is granted to any school ICT resource.
 - Access to the Internet will be by adult demonstration initially with supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return the 'Pupils Code of Conduct' before access is granted.
- Parents will be informed that pupils will be provided with supervised Internet access.

4.2 How will risks be assessed?

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

- 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, BucksCC nor Turn It On 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 How will E-Safety complaints be handled?

- Pupils and parents will be informed of the complaints procedure.

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.

4.4 How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to E-Safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

5. Communicating the Policy

5.1 How will the policy be introduced to pupils?

- Pupil's Internet Code of Practice will be posted in rooms with Internet access. A copy is available via the school website.
- Pupils will be informed that network and Internet use will be monitored.
- An E-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- An E-Safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.
- Instruction in responsible and safe use will precede Internet access.

5.2 How will the policy be discussed with staff?

- The E-Safety Policy has been discussed at staff meetings and is kept in the Policy Folder.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Any issues with internet use identified by the filtering system are reported to the Computing Co-ordinator who will liaise with senior management and Turn It On.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, the school prospectus and on the school website.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in **(Appendix 1)**- E-Safety Contacts and References.

(Appendix 1)

E-Safety Contacts and References

National Online Safety

<https://nationalonlinesafety.com/> (we are members of this organisation and parents can log in to access materials)

BucksGfL Website

<http://www.bucksgfl.org.uk>

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/>

Kidsmart

<http://www.kidsmart.org.uk/>

NSPCC

<http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm>

Think U Know website

<http://www.thinkuknow.co.uk/>

Virtual Global Taskforce – Report Abuse

<http://www.virtualglobaltaskforce.com/>

(Appendix 2)

Computer Resources Policy Pupil Guidelines

The school has provided computers for use by you. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all. You are encouraged to use and enjoy these resources, and ensure they remain available to all. You are responsible for good behaviour on the Internet as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not open files brought in on removable media (such as, CDs, flash drives, memory sticks etc.) until they have been checked with antivirus software by the ICT coordinator.
- Do not eat or drink near computer equipment.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so by a teacher.
- Do not use the computers in a way that harasses harms, offends or insults others.
- Do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and memory sticks will be treated like school lockers. Teachers may review files and communications to ensure that users are using the system responsibly.

Internet/World Wide Web

- Do not access the Internet unless for study or for school authorised / supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, racist, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.
- Political indoctrination of staff or pupils by self-radicalisation or extremist views is not accepted.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

