



Policy for Online Safety and Internet Use

Reviewed by: Mrs J Apostol

Date: 20 January 2025

Review Date: January 2026

Adopted by
Governing Body: January 2025

Amendments		
Date	Action	Signed
November 2022	Update according to KCSIE and wider knowledge and advice Pupils to read, agree and sign internet use agreement	J.Apostol
November 2024	Update according to KCSIE and wider knowledge and advice Pupils to read, agree and sign internet use agreement	J.Apostol
January 2025	Re-design internet use posters to each classroom	J.Apostol

1 The purpose of this policy statement

1.1 The Internet is now regarded as an essential resource to support teaching and learning across the curriculum. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT.

1.2 In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning, such as ipads. Computer skills are vital to access life-long learning and employment; ICT is an essential life-skill.

1.3 Young people have access to the Internet from many places, home, school, friends' homes and in most cases mobile devices. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become internet safe. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home through regular online safety units of work, assemblies and classroom discussions.

2 Core Principles of Online Safety:

2.1 Online safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

2.2 It must be remembered that there are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant and responsible.

3 The Internet:

3.1 Why Internet use is important:

'Digital technology is driving extraordinary global changes that some are calling the Fourth Industrial Revolution. Navigating these changes effectively and safely requires a significant understanding of digital literacy, information technology and computer science. This knowledge is also crucial if business, industry and individuals are to exploit the opportunities offered by this revolution. The national curriculum makes it clear that computing is mandatory at key stages 1 to 4 and that 'a high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world.'

- The school has a duty to provide pupils 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, well being and to support the professional work of staff and to enhance the school's management information and business administration systems.

3.2 How Internet use enhances learning:

- The school Internet access will be designed for educational use and will include filtering appropriate to the age of pupils through Warwickshire Education Services.
- Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
- Pupils will be educated in the effective use of internet research which is age appropriate.

3.3 How Internet access is authorised:

- The school will keep a record of all staff and pupils who are granted Internet access.
- Parents will be informed that pupils will be provided with supervised Internet access whilst on school site.
- Children are given online safety agreements from Year 1 to Year 6, which they must read and sign; it is the teachers' duty to ensure the children's understanding of the terms. These agreements need to be reviewed with the children each year and any new pupils must also read, understand and sign the agreement.

3.4 How filtering is managed:

- The school will work in partnership with parents and Warwickshire County Council (ICTDS).
- If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing lead/headteacher. Parents of the children involved will be notified.
- Website logs will be regularly sampled and monitored.
- Computing lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.5 How risks are assessed:

- In common with other media such as television, magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher and Computing lead will ensure that the Online Safety Policy is implemented and compliant with the policy monitored.

3.6 How pupils and staff learn to evaluate Internet content:

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing lead and the ICTDS (01926414100)
- Specific lessons will be included within the ICT Scheme of Work that teaches all pupils how to read for information from web resources.
- Nominated persons (ICTDS) will be responsible for permitting and denying additional websites as requested by colleagues.
- Children will be trained and regularly reminded to use appropriate strategies if inappropriate content appears on their screen. (Screen off, tell the nearest adult) This is the responsibility of the ICT coordinator to ensure the children are aware of what to do in such circumstances. This should be delivered during assemblies by the ICT coordinator relevant to KS1 and KS2 at the beginning of each half term.
- Staff to use SharePoint to store documents/data which is supplied/backed up by ICTDS, to ensure security.

3.7 How the school website/Facebook/Instagram/Twitter content is managed:

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Social media photographs that include pupils will be selected carefully (those who have been granted permission by parents) and will not enable individual pupils to be identified by name.
- Pupils' full names will not be used anywhere on social media.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media.

4 Communication

4.1 Managing e-mail

- Pupils may only use approved e-mail accounts on the school system through their individual Purple Mash accounts. This is a child friendly system which is monitored during school hours through ICTDS.
- Pupils must immediately tell a teacher if they receive offensive e-mails from other pupils.
- Pupils must not send emails to anyone outside of the Purple Mash platform.
- Pupils should only send emails to the teacher, or other pupils, when asked to do so by their teacher when on school site.

4.2 On-line communications and social networking.

- Pupils will be taught about how to keep personal information safe when using online services.
- Pupils will be educated on age restrictions of apps/programs/games/social media sites and discuss the safety reasons why these restrictions may apply, but will also teach the pupils how to set security settings to ensure they are using it as safely as possible.
- Each year group will have a dedicated session in 'classroom teacher assemblies' using Project Evolve to allow the pupils an opportunity to discuss online safety 'at home.' This might include: What's App and shared messaging, the use of online gaming, social media, posting photographs, ensuring children feel confident to talk to their parents when issues/inappropriate content arises.

4.3 Mobile technologies

- Appropriate use of mobile phones will be taught to pupils as part of their online safety program.
- Pupil mobile phones are not permitted within the school. Only Y6 pupils, who need to bring phones to school (if going between two parental homes) must hand their phone into their teacher to store during school hours. They must not use this

device at all when on school site and they must not link their device onto the school network.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. (A Switch might be used for a class by use of the teacher, but this must be agreed by the Computing Lead)

5 Introducing the Policy to Pupils and Parents

- Rules for Internet access will be posted in all rooms where computers are used.
- A unit within the Purple Mash scheme of work on responsible Internet use and online safety will be included in the curriculum in each year group 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 should precede Internet access.
- Pupils will be informed that Internet use will be monitored.
- Parents' attention will be drawn to the School Online Safety messages in newsletters and on the school Website.
- Regular information will be provided to parents 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 without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.