

E-Safety Policy



Status	Date
Date issued	October 2024
Prepared by	Stephen Harvey
Review date	September 2026
Date adopted by Governing Body	November 2024

Together, we nurture, inspire and achieve

Introduction

In an increasingly digital world, it is essential for students to navigate online environments safely and responsibly. This E-safety policy outlines our approach to promoting safe online practices among students, staff, and parents, aligning with the expectations set forth by Ofsted and the 2014 National Curriculum in England.

Aims

The aims of this E-safety policy are to:

- Safeguard children from potential online risks, including cyberbullying, inappropriate content, and online predators.
- Equip students with the knowledge and skills to use digital technology safely and responsibly.
- Promote a whole-school approach to E-safety, involving staff, parents, and the wider community.
- Ensure compliance with relevant legislation and guidance on E-safety, including the Children Act 1989 and the UK General Data Protection Regulation (GDPR).
- Foster digital citizenship by encouraging respectful and responsible online behaviour.

Scope

This policy applies to all members of the school community, including students, staff, parents, and visitors, who use technology within the school environment or in relation to school activities. The policy encompasses all forms of digital communication, including social media, emails, messaging apps, and online gaming.

E-safety Education

Curriculum Integration

- **Teaching E-safety:** E-safety will be integrated into the curriculum across all subjects, particularly within Computing, PSHE, and Citizenship education. Each key stage will involve age-appropriate lessons that address online risks, digital citizenship, and responsible technology use.
- **Digital Literacy:** Students will develop skills in digital literacy, which include understanding acceptable online conduct, recognising misinformation, and knowing how to report online issues.

Age-Appropriate Guidance

- **Foundation Stage:** Introduction to appropriate online behaviours through stories, role-play activities, and discussions about safe technology use.
- **Key Stage 1:** Teaching basic understanding of the internet, the importance of strong passwords, identifying trusted adults for online safety, and recognising safe versus unsafe content.

- Key Stage 2: More in-depth discussions on social media etiquette, the implications of sharing personal information, cyberbullying prevention strategies, and the significance of digital footprints.

Roles and Responsibilities

- Computing Subject Leader: Responsible for the development and implementation of the E-safety policy, providing ongoing training for staff, conducting E-safety audits, and partnering with local authorities for resources and support.
- Staff Members: All staff must model safe online behaviour, lead E-safety discussions, integrate E-safety practices into lessons, and report any incidents of misuse or inappropriate behaviour.
- Parents and Carers: Parents are encouraged to engage with the school's E-safety initiatives, to support their child's online activities at home, and to attend information sessions to learn more about emerging online risks and safety measures.

Policy Implementation

Acceptable Use Agreement

- A comprehensive Acceptable Use Agreement will be established for students, parents, and staff. This includes clear guidelines on acceptable online behaviour, responsibilities, accountability measures, and consequences for breaches of policy.
- This agreement will be revisited annually, ensuring that it reflects current online safety standards and practices.

Online Safety Procedures

- Regular audits of online safety measures within the school, including comprehensive reviews of internet filtering solutions, firewall security, and monitoring processes to ensure compliance with standards.
- Incident reporting procedures for incidents of cyberbullying, misuse of technology, or data breaches will be clearly defined, ensuring that students feel comfortable reporting issues confidentially.

Training and Development

- Regular E-safety training for staff will be conducted at the beginning of each school year and supplemented through ongoing professional development opportunities.
- Information sessions and workshops for parents will run periodically, promoting awareness of online safety resources, age-appropriate technology management, and strategies for supporting children's online interactions.

Monitoring and Review

- The E-safety policy will be reviewed annually in consultation with stakeholders, including staff, students, and parents, ensuring its effectiveness and alignment with current digital trends.

- Monitoring of the effectiveness of training and educational outcomes will be carried out through surveys, feedback sessions, and the analysis of reported incidents.

Summary of Expectations According to Ofsted Framework

According to the latest Ofsted framework, outstanding schools should:

- Demonstrate a clear strategy for E-safety that is integrated into the school culture and reflects the diverse needs of the school community.
- Provide comprehensive training for staff and robust learning opportunities for students regarding online safety, ensuring that it is a collaborative effort across all subjects.
- Involve parents in E-safety awareness and education activities, ensuring they are informed and equipped to support their children at home.
- Monitor and evaluate the effectiveness of E-safety policies and practices regularly through active engagement with the school community, making necessary adjustments based on feedback and emerging trends.

Conclusion

This E-safety policy reflects our commitment to safeguarding students and fostering a safe online learning environment. It will evolve with technology and the needs of our school community, ensuring that all members are well-equipped to use digital resources responsibly and safely.