E-Safety is about enabling the school community to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life. It is not just about the risks, and how we avoid them; it is about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities.
E-Safety depends on effective practice at a number of levels:
• Responsible ICT use by all staff and students; 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 and the effective management of content filtering.
• National Education Network standards and specifications.

An E-Safety policy allows the school to demonstrate that not only do we acknowledge E-Safety as an important issue for the school community, but also that we have made a considered attempt to embed E-Safety into our approach to learning using technology.
An E-Safety policy demonstrates how we have worked to achieve a balance between using technology to enhance learning and teaching, and putting appropriate safeguards in place. The school's E-Safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student 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 students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access.
Students will use the Internet outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:
• Access to learning wherever and whenever convenient.
• 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 students world-wide.
Access to experts in many fields for students 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 DCSF.

How Can Internet Use Enhance Learning?

• The school Internet access is designed expressly for student use and includes filtering appropriate to the age of students.
• Students 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 will guide students in on line activities that will support learning outcomes planned for the students' age and maturity.
• Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Head teacher

• Develop and promote an E-Safety culture within the school community.
• Support the E-Safety co-ordinator in their work.
• Make appropriate resources, training and support available to members of the school community to ensure that they are able to carry out their roles with regard to E-Safety effectively.
• Receive and regularly review E-Safety incident logs and be aware of the procedure to be followed should an E-Safety incident occur in school.
• Take ultimate responsibility for the E-Safety of the school community.
• Promote an awareness and commitment to E-Safety throughout the school.
• Be the first point of contact in school on all E-Safety matters.
• Create and maintain E-Safety policies and procedures.
• Develop an understanding of current E-Safety issues, guidance and appropriate legislation.
• Ensure all members of staff receive an appropriate level of training in E-Safety issues.
• Ensure that E-Safety education is embedded across the curriculum.
• Ensure that E-Safety is promoted to parents and carers.
• Monitor and report on E-Safety issues to Senior Leadership Team as appropriate.
• Ensure an E-Safety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff

• Read, understand and help promote the school's E-Safety policies and guidance.
• Read, understand and adhere to the school staff Acceptable Usage Policy.
• Develop and maintain an awareness of current E-Safety issues and guidance.
• Model safe and responsible behaviours in their own use of technology.
• Embed E-Safety messages in learning activities where appropriate.
• Supervise pupils carefully when engaged in learning activities involving technology.
• Be aware of what to do if an E-Safety incident occurs.
• Maintain a professional level of conduct in their personal use of technology at all times.
• To pass on details of any E-Safety incidents to be logged by the E-Safety co-ordinator.

Responsibilities of Pupils

• Read, understand and adhere to the school pupil Acceptable Usage Policy.
• Help and support the school in creating E-Safety policies and practices; and adhere to any policies and practices the school creates.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies in the school and at home.
• Take responsibility for their own and other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of the school.
• Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in the school and at home.
• Understand what action to take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in the school and at home, or if they know of someone who this is happening to.
• Discuss E-Safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

• Help and support the school in promoting E-Safety.
• Read, understand and promote the school pupil Acceptable Usage Policy with their children.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in school and at home.
• Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
• Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
• Model safe and responsible behaviours in their own use of technology.
• Consult with the school if they have any concerns about their children's use of technology.

Responsibilities of Operations Director and Directors

• Read, understand, contribute to and help promote the school's policies and guidance.
• Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
• Develop an overview of how the school ICT infrastructure provides safe access to the Internet.

• Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
• Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.
• We will provide a series of specific E-Safety-related lessons as part of the ICT / Computing curriculum and PSHCE curriculum.
• We will celebrate and promote E-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
• We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
• School will ensure that the use of Internet derived materials by students and staff complies with copyright law.
• Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
• We will remind pupils about their responsibilities through an end-user Acceptable Usage Policy which will be displayed throughout the school and have to be accepted each time a pupil logs on.
• Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:
• include useful links and advice on E-Safety on our school website;
• provide parents with useful information from the ThinkUKnow and ChildNet websites.

Managing ICT Systems and Access

• The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
• Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
• Servers, workstations and other hardware and software will be kept updated as appropriate.
• Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
• The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
• All users will agree with an end-user Acceptable Use Policy appropriate to their age and access before joining the school as part of the home-school agreement and each time they log on to the school network.
• Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school ICT systems and that such activity will be monitored and checked.
• Pupils will access the Internet using an individual log-on, which they will keep secure. Whether supervised by a member of staff, or working independently, pupils will abide by the school Acceptable Usage Policy at all times.

• Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school Acceptable Usage Policy at all times.
• Any administrator or master passwords for school ICT systems will be kept secure.

Wireless Access

• Wireless access to the network is provided in certain areas of the school. The school is responsible for ensuring that access is as safe and secure as is reasonably possible.
• Connection to the wireless network is protected by at least the Wi-Fi Protected Access (WPA) authentication method requiring the input of a secure passphrase.

Inappropriate content

• The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
• The school will regularly audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

• The school uses a filtered Internet service. The filtering is provided by the school using third party filter lists provided.
• If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the ICT Services Department.
• If users discover a website with potentially illegal content, this should be reported immediately to the Head teacher. The school will report this to appropriate agencies including the filtering provider, Local Authority, Child Exploitation & Online Protection Centre (CEOP) or Internet Watch Foundation (IWF).
• The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning technologies in school

Using email

• Staff should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.

Using mobile phones

• Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone should be provided and used. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Using new technologies

• As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.
• We will regularly amend the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safety risk.

Protecting personal data

• We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
• Staff will ensure they properly log-off from a computer terminal after accessing personal data.
• Staff will not remove personal or sensitive data from the school premises without permission of the head teacher, and without ensuring such data is kept secure.
• All staff will be aware of and have access to the Data Protection policy.

The school website and other online content published by the school

• The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
• A generic contact e-mail address will be used for all enquiries received through the school website.
• All content included on the school website will be approved by the Directors.
• The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
• Staff and pupils should not post school-related content on any external website without seeking permission first.

Communication of Policy

Pupils

• The pupil Acceptable Usage Policy will be displayed in school areas and must be accepted before logging on to the network.
• 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.
• Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

Parents

• Parents/Carers' attention will be drawn to the school E-Safety Policy and Acceptable Usage Policy in the school prospectus and on the school website.

Dealing with breaches of ICT Policy

• accessing illegal content deliberately
• accessing inappropriate content deliberately
• accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time
• sharing your username and password with others
• opening, altering, deleting or otherwise accessing files or data belonging to someone else
• failure to abide by copyright of licensing agreement

Whilst resolving an incident those students involved may have their computer accounts suspended.
Examples of possible E-Safety incidents involving pupils:
• accessing illegal content accidentally and failing to report this
• accessing inappropriate content accidentally and failing to report this
• inappropriate use of personal technologies (e.g. mobile phones) at school
• accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed
• downloading or uploading files not allowed
• accessing school ICT systems with someone else's username and password
• using school or personal equipment to send a message, or create content, that is offensive or bullying in nature
• attempting to circumvent school filtering, monitoring or other security systems
• sending messages, or creating content, that could bring the school into disrepute
• revealing the personal information (including digital images, videos and text) of others by electronic means (e.g., sending of messages, creating online content) without permission
• use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content).

Examples of possible E-Safety incidents involving staff:

• transferring personal data insecurely

• using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)

Where a member of staff is made aware of a possible E-Safety incident, they should inform Head teacher who will then use the schools agreed procedure to respond in the most appropriate manner.