



**Health
Futures**
UTC

E safety Policy



Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

This policy has been strongly influenced by the work of the e-Safety team.

End to End e-Safety

E-Safety depends on effective practice at many 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 including the effective management of filtering systems

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

- The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection.
- The school's e-Safety Co-ordinator is also **Annette Guest**. She works in close co-operation with the principal and senior leadership team. These staff are the Designated Child Protection Officers
- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- E-Safety issues are included in the Child Protection, Health and Safety, Anti- Bullying, and ICT policies.
- The e-Safety Policy will be reviewed March 2019

1.2 Teaching and learning

1.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

1.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for student use and will include 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 should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Students will be taught how to evaluate Internet content

- If staff or students discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator/Network manager/e-safety officer.
- Staff should ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

1.3.2 E-mail

- Students may only use approved e-mail accounts on the school system. Students are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation 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.

1.3.3 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 student's personal information will not be published.
- The principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Student's work can only be published with the permission of the student and parents.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Students and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged students.

1.3.6 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or students discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 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.

- **Internet enabled devices will not be used during lessons.** The sending of abusive or inappropriate text messages is forbidden.
- Staff have access to a school phone where contact with students is required.

1.3.8 Protecting personal data

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

1.4 Policy Decisions

1.4.1 Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. 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. The school can accept liability for the material accessed, or any consequences of Internet access.

- The principal will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.2 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Sanctions within the school discipline policy include: – interview/counselling by class teacher / principal; – informing parents or carers; – removal of Internet or computer access for a period.

1.4.3 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to students

- Rules for Internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

1.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

1.5.3 Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy via school website or in newsletters.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Students should be supervised. Students should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Students should be supervised. Students should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Picsearch safesearch NOT Google images
Exchanging information with other students and asking questions of experts via e-mail.	Students should only use approved e-mail accounts. Students should never give out personal information. Consider using systems that provide online moderation e.g. Super Clubs.	GridClub School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing students' work on school and other websites	Student and parental consent should be sought prior to publication. Students' full names and other personal information should be omitted.	School website Learn Premium Espresso
Publishing images including Photographs of students.	Parental consent for publication of photographs should be sought. Photographs should not enable individual students to be identified. File names should not refer to the student by name.	School website
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used.	GridClub

	Access to other social networking sites should be blocked. Students should never give out personal information.	
Audio and video conferencing to gather information and share students' work.	Students should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	City Learning Centres

E-Safety Audit

This quick audit will help the senior management team (SMT) assess whether the basics of e-Safety are in place **to support a range of activities that might include those detailed within Appendix 1.**

The school has an e-Safety Policy	Yes
Date of latest update:	March 2018
The Policy was agreed by governors on:	Y/N
The Policy is available for staff	Yes
And for parents	Yes Internet
The Designated Child Protection Coordinator is	Matt Bradley
The e-Safety Coordinator is	Annette Guest
How is e-Safety training provided? Explain:	Staff Inset training
Is the EPICT training available to staff? M Waller completed training and is a facilitator.	M Waller
All staff sign an Acceptable ICT Use Agreement.	Y
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	Y
Rules for Responsible Use have been set for students:	Y

Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of LT.	Yes