



Name of Policy:

E-Safety and Acceptable Use Policy

Reviewed Edition	September 2019
Next Review	September 2020
Person responsible for updating policy	KS/SLT
Governors Committee responsible	CURRICULUUM

Contents

Writing and reviewing the E-safety policy.....	3
Teaching and learning	3
Why Internet and digital communications are important	3
Pupils will be taught how to evaluate Internet content	3
Managing Internet Access	3
Information system security	3
E-mail.....	3
Published content and the school web site	4
Publishing pupils’ images and work	4
Social networking and personal publishing on the school learning platform.....	4
Managing filtering	4
Managing videoconferencing.....	4
Managing emerging technologies.....	5
Protecting personal data.....	5
Policy Decisions	5
Authorising Internet access.....	5
Assessing risks	5
Handling E-safety complaints.....	5
Community use of the Internet.....	5
Communications Policy	6
Introducing the E-safety policy to pupils	6
Staff and the E-safety policy.....	6
Enlisting parents’ support	6

Writing and reviewing the E-safety policy

- The school's appointed E-safety coordinators are the **Head teacher** and the **Computing subject leader**.
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management.
- The E-safety Policy and its implementation will be reviewed annually.
- The E-safety Policy was revised on 22/9/2017.

Teaching and learning

Why Internet and digital communications are 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 pupils. Children are encouraged to use the internet as a resource when carrying out research work across the curriculum, for both home and school work.
- The school Internet access is provided by a **Talk Straight** contract and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, evaluation and filtering.
- Pupils are shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school seeks to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- ***Pupils are taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or the Think the Click initiative.***

Managing Internet Access

Information system security

- School ICT systems security are reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the Local Authority.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

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 pupils' personal information are not to be published.
- The **Head teacher** takes overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully. The school seeks to use group photographs rather than full-face photos of individual children.
- Pupils' full names should be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers are checked and/or obtained before photographs of pupils are published on the school Web site.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school controls access to social networking sites, and considers how to educate pupils in their safe use e.g. use of passwords.
- Pupils are advised never to give out personal details, whether their own or belonging to other people, of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils are advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school works in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator.
- Senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing can use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils will only be involved in a video conference if an adult is present with them.
- Videoconferencing is appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones and associated cameras are not permitted during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff should use a school phone where contact with pupils is required.
- The appropriate use of Learning Platforms is discussed as the technology becomes available within the school.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- Parents are asked to sign and return a consent form at the beginning of their child's formal education within the school.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
The school regularly audits ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents should be aware of the complaints procedure.
- Pupils and parents have been informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations should be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy is shared with pupils.
- E-safety rules are posted in suitable locations, for example the ICT suite.
- Pupils are informed that network and Internet use are monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them are provided for pupils when applicable.

Staff and the E-safety policy

- All staff have been 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.
- Staff that manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention is drawn to the School E-safety Policy by regular announcements in newsletters, the school brochure and on the school web site.
- Parents and carers are from time to time provided with additional information on E-safety.
- The school asks all new parents to sign the parent/pupil agreement when they register their child with the school.