# St Augustine of Canterbury

# e-Safety Policy

## Overview

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 pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

Our e-Safety Policy has been written by the school, building on government guidance.

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

The school's ICT subject leader will also act as the e-Safety Coordinator.

## 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 pupils.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

## Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable, and what is not, and will be given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, filter and evaluation.

Pupils in the infant and lower junior classes will not be allowed to 'free-surf' the web. Internet access for these pupils will be done by staff providing a selection of evaluated sites which can be accessed through the school's VLE.

## Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

## Information system security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with the LA and updated regularly.

## E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail or emails from an unknown party.
- Pupils must not reveal personal details (including, address, telephone numbers) of themselves or others in e-mail communication.
- Pupils must not arrange a meeting through email communication.
- The forwarding of chain letters is not permitted.
- Education about email safety will be covered in the eSafety provision for parents, staff and pupils.

## Published content and the school Website

The contact details on the Web site should be the school address, e-mail and telephone number. Staff, Governor or pupils' personal information will not be published.

The ICT coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site or VLE, in association with photographs.

Written permission from parents or carers will be obtained on the pupil's entry to school and before photographs of pupils are published on the school Web site.

Pupil's work can only be published with the permission of the pupil and parents – permission for this is gained on pupils admission.
Parents will be notified at all public performances about the confidential use of images in respect of social networking sites.

## Social networking and personal publishing

The school will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that the use of social network spaces such as Facebook, MySpace and Bebo outside of school is inappropriate for primary aged pupils. They will also be advised of the benefits and dangers of other social networking sites intended for Primary age pupils such as Club Penguins and Moshi Monsters. They will also be offered specific guidance, through e-safety workshops, on how they can best keep their children safe should they permit use at home.

## Managing filtering

The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is inappropriate will be reported to appropriate agencies.

Parents will be advised upon the importance of filtering on home computers at the annual e-Safety workshop.

## Managing video conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

### 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.

Mobile phones will not be used during lessons or formal school time. Mobile phones should be handed to the teacher in charge during the school day.

Teachers will contact parents using a text message service when the need occurs eg. school closures, cancellation of after school activities, reminders about meetings and events.
Parents should not contact staff through text messaging.

### Protecting personal data

Personal data will be 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 'AUP' before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. Parents will be given a copy of the AUP which governs ICT use in school as their child enters school. KS2 pupils will be required to sign the AUP each year as part of e-Safety lessons.

### Assessing risks

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. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

### 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 Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Parents and pupils will need to work in partnership with staff to resolve issues.

# Communications Policy

## Introducing the e-safety policy to pupils

E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

Pupils in all classes will receive specific e-safety lessons each term.

Pupils will be expected to adhere to the AUP and KS2 pupils will sign a copy of this each year in e-Safety lessons

## 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.

Staff training in safe and responsible Internet use and on the school e-safety policy will be provided as required.

## Parents'

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site at regular intervals throughout the school year.

An e-safety meeting / workshop will be held annually to review parent concerns, address emerging technologies and educate parents about e-safety issues.

Internet issues will be handled sensitively, and parents will be advised accordingly.

**Review Date: Autumn 2016**