

**ICT POLICY INCORPORATING E-SAFETY
(Whole School)**

RATIONALE

ICS understands the great power inherent in modern technology and appreciates that a truly connected world can only exist through technology. With that power comes responsibility. Our starting point with our students, which is reinforced through the education provided at ICS, is that they understand where the boundaries of appropriate uses of technology lie. Respecting others is at the heart of our philosophy and extends into the digital domain. These boundaries however are changing as familiarisation with new forms of communication develop. If lines are crossed, then, within the secure environment of a small, community based school, a serious learning opportunity will arise.

ICS recognises that the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, collaboration, stimulate global awareness and enhance learning.

As part of our commitment to learning and achievement, we at ICS want to ensure that the Internet and other digital technologies are used to:

- raise educational standards and promote student achievements;
- develop the curriculum and make learning exciting and purposeful;
- enable students to gain access to a wide span of knowledge in a way that ensures their safety and security;
- develop students' skills of cooperation, collaboration and competition;
- prepare our students to be effective 21st Century citizens.

The school's ICT policy will operate in conjunction with other policies including those for Student Behaviour and Sanctions, Child Protection and Curriculum.

Scope of Policy

The policy applies to:

- all students;
- all teaching and support staff and volunteers;
- all aspects of the school's facilities where they are used by voluntary, statutory or community organisations.

ICS will ensure that the following elements are in place as part of its safeguarding responsibilities to students:

- staff who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;

- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of students when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- a reporting procedure for abuse and misuse.

ICS expects all staff and students to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below.

Users should not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to the promotion of illegal acts. In addition, all computer use should be mindful of the school philosophy, and respectful of the diverse and inclusive community which ICS is made up of.

1. Teaching and learning

1.1 Why Internet use is important

The Internet is an essential element in 21st Century life for education, collaboration, 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.

1.2 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.

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

1.3 Students will be taught how to evaluate Internet content

The school 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.

2. Managing Internet Access

2.1 Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be installed and updated regularly.

Security strategies will be discussed with the network manager.

2.2 E-mail

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 from a supervising adult.

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.

2.3 Published content and the school web site

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

A nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupils' images and work

Students' full names will not be used anywhere on the website or blog, particularly in association with photographs.

Written permission from parents or carers is obtained before photographs of students are published on the school website.

2.5 Social networking and personal publishing

School will block/filter access to social networking sites at school computers.

Newsgroups will be blocked unless a specific use is approved

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

Students must not place personal photos on any social network space.

Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

2.6 Managing filtering

The school will work in partnership with the Internet Service Provider to ensure systems to protect students are reviewed and improved.

If staff or students discover an unsuitable site, it must be reported to the ICT Network Manager.

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

2.7 Managing videoconferencing

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

Videoconferencing will be appropriately supervised for the students' age.

2.8 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.

The sending of abusive or inappropriate text messages is forbidden.

2.9 Protecting personal data

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

3. Policy Decisions

3.1 Authorising Internet access

The school will maintain a current record of all staff and students who are granted access to school ICT systems.

Students must apply for online access individually by agreeing to comply with the relevant Acceptable Use Policy.

Parents will be asked to sign and return a consent form for loaning wireless Netbooks.

3.2 Assessing risks

The school will take 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 student netbook. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the measures to address e-safety are adequate and that the implementation of these measures is appropriate.

3.3 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 of school.

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.

4. Communications Strategy

4.1 Introducing e-safety to students

Students will sign a code of conduct for using Netbooks, the Internet and the school ICT systems.

E-safety rules will be posted in all networked rooms.

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

4.2 Staff and e-Safety

All staff will be given the school e-Safety measures and their 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 will be supervised by senior management and have clear procedures for reporting issues.

4.3 Enlisting parents' support

Parents' attention will be drawn to the school ICT Policy on the school website.

4.4 Reporting Abuse

There may be occasions when either a student or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the student or adult should report the incident **immediately**.

5. Monitoring

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a student or member of staff may have. ICS recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school.

With regard to monitoring trends, within the school and individual use by school staff and students, ICS will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school will include the monitoring of content and resources.

Another aspect of monitoring, which our school will employ, is the use of mobile technologies by students, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our students, and where necessary, support individual students where they have been deliberately or inadvertently been subject to harm.

6. Sanctions

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

- Child / Young Person
 - The child/young person will be disciplined according to the Behaviour and Sanctions Policy of the school, which could ultimately include the use of Internet and email being withdrawn.
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- Adult (Staff and Volunteers)
 - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy.
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

If inappropriate material is accessed, users are required to immediately report this to the Senior Management Team so this can be taken into account for monitoring purposes.

7. E-safety Appendices

There are multiple aspects of the school's E-safety measures, which incorporate acceptable use for both staff and pupils; ICT equipment (onsite and offsite); data security and retention.

Appendix 1: Student Code of Conduct for using Netbooks
Appendix 2: Student ICT Code of Conduct
Appendix 3: Staff ICT Code of Conduct

Updated: December 2010
Review Date: December 2011