eSAFETY POLICY

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour, Child Protection and Mobile Phone Use.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

1. INTRODUCTION

Boards of Governors have a duty to safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries (Northern Ireland)
Order 2003). It is also the duty of the Board of Governors to determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003 refers).
In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.
This E-safety policy is largely based on DENI Circular 2007/1 *"Acceptable Use of the Internet and Digital Technologies in Schools",* DENI Circular 2011/12 "*Internet Safety*" and DENI Circular 2013/2015 "*eSafety Guidance*", and should also be read in conjunction with the School's Child Protection Policy.

2. INTERNET SAFETY POLICY

The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. Holy Cross College provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.
The DENI circular 2007/01 states that:
"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."
This document sets out the policy and practices for the safe and effective use of the internet in Holy Cross College. The policy has been drawn up by the Head of ICT under the leadership of the Principal and Senior Management Team. It has been approved by the Board of Governors, communicated to and agreed by all staff and is available to all parents as a hard copy, if requested.
The policy and its implementation will be reviewed annually.

3. MY-SCHOOL

MY-SCHOOL is the project responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

Some of these safety services include:

- Providing all users with a unique user name and password;
- Tracking and recording all online activity using the unique user name and password;
- Scanning all MY-SCHOOL email and attachments for inappropriate content and viruses;
- Filters access to web sites;
- Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than My-SCHOOL then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place. Currently Holy Cross College has no plans to access any online services outside of MY-SCHOOL.

4. Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. We have a Code of Safe Practice (Appendix A) for pupils and staff containing eSafety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, iPads, PDAs) is subject to the same requirements as technology provided by the school.

The Head of ICT and the Principal/Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

The code of practice with a parental consent slip (Appendix A and B) is sent out annually to parents/carers and this consent must be obtained before the pupil accesses the internet.

In addition, the following key measures have been adopted by Holy Cross College to ensure our pupils do not access any inappropriate material:

- The school's eSafety code of practice for Use of the Internet and other digital technologies is made explicit to all pupils and eSafety guidelines are displayed prominently throughout the school;
- Our Code of Practice is reviewed each school year and signed by parents. It is included in the Student Planner, Key Stage 3/4;
- Pupils using the Internet will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils in all key stages are educated in the safe and effective use of the Internet, through a number of selected websites.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor MY-SCHOOL can accept liability under such circumstances.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Behaviour Policy. Incidents involving child protection issues will be dealt with in accordance with the school's Child Protection Policy.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with teaching staff and support staff:

- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils;
- All pupils using the Internet have written permission from their parents;
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/Head of ICT;
- In the interests of system security staff passwords should only be shared with the ICT technician and Head of ICT;
- Teachers are aware that the MY-SCHOOL system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users;
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these;
- Photographs of pupils should, where possible, be taken with a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work;
- School systems may not be used for unauthorised commercial transactions.

5. Internet Safety Awareness

In Holy Cross College we believe that, alongside having a written eSafety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms.

Internet Safety Awareness for staff

The Head of ICT keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Departments policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.
The Child Exploitation and Online Protection Centre (CEOP) **runs regular one-day courses for teachers in Northern Ireland. These are advertised directly to schools. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the** Thinkuknow website**.**

Internet Safety Awareness for parents

The Internet Safety Policy and Code of safe Practice for pupils is sent home at the start of each school year for parental signature. Additional advice for parents with internet access at home is also distributed for pupils in Year 8 (Appendix C)

Community Use of School ICT Resources

The school's ICT facilities are used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by MY-SCHOOL. They must also agree to the school's Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

6. Health and Safety

In Holy Cross College we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, in classrooms and in both of the ICT suites, which have been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors.

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available at: the Health Protection Agency website.

7. School Web Site

The school web site is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well presented

and that personal security is not compromised. As the school's web site can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff.
The following rules apply:

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published;
- Web site photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site;
- The Website Administrator will take overall editorial responsibility and ensure that content is accurate and appropriate;
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

8. Social Software

This is a generic term for community networks, chatrooms, instant messenger systems, online journals, social networks and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.
The majority of activity in these on-line social sites usually causes no concern. My-SCHOOL filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment.
We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Appropriate information and indeed education will also be provided for our parents.
Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's discipline policy and child protection procedures.
Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.
Holy Cross College has a Facebook page which is updated regularly with school news, PTA events and any fundraising/charity initiatives the school is involved with. MY-SCHOOL access to the school Facebook page is available to one member of the school's admin team for the purposes of updating the page during school opening hours.

Appendix A CODE OF PRACTICE FOR USING THE INTERNET

When using the Internet, all users, staff and pupils, must comply with all copyright, libel, fraud, discrimination and obscenity laws.
Pupils are responsible for their good behaviour on the school network just as they are on and off the school premises. While the use of ICT is a requirement of the Northern Ireland Curriculum, access to the Internet is a privilege and not a right and therefore should not be abused. It is given to pupils who act in a considerate and responsible manner, and will be withdrawn if they fail to maintain acceptable standards of use.

No internet user is permitted to:

- Retrieve, send, copy or display offensive messages or pictures;
- Use obscene or racist language;
- Harass, insult or attack others;
- Damage computers, computer systems or computer networks;
- Violate copyright laws;
- Use another user's password;
- Trespass in another user's folders, work or files;
- Intentionally waste resources (such as on-line time and paper);
- Use the network for unapproved commercial purposes.

Users should be aware that the school can and does track and record the sites visited and searches made on the Internet and e-mails sent and received to maintain system integrity and ensure users are using the system responsibly.
While using the Internet in school, pupils should be supervised where possible. When appropriate, pupils may carry out independent research if they have been given permission.

Examples of acceptable use

- The use of e-mail, video and computer conferencing for communication between colleagues, pupils, teachers, schools and industry;
- The use of the internet to research school subjects; cross-curricular themes and topics related to social and personal development;
- The use of the Internet to investigate careers and further education;
- The development of pupils' competence in ICT skills and their general research skills;

*Examples of activities which are **not permitted** include:*

- Searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- Copying, saving or redistributing copyright protected material, without approval;
- Subscribing to any services or ordering goods or services, unless specifically approved by the school;
- Playing computer games or using other interactive "chat" sites, unless assigned by the teacher;
- Using the network in such a way as to disrupt it for other users, e.g. downloading large files or software i.e. screen savers, wallpaper, sending mass e-mail messages);
- Publishing, sharing or distributing any personal information about a user, such as address, phone number;
- Any activity that violates a school rule.

While the school provides a filtered Internet service provided by MY-SCHOOL, it should be noted that no service can be totally secure and pupils are required to report any offensive material they encounter on the network.
Pupils should be aware that their use of the Internet is monitored and that action will be taken to counter any abuse.

Appendix B

We have discussed the Code Practice and ……………………………………......... (child's name) agrees to follow the eSafety rules and to support the safe use of ICT at Holy Cross College.

Parent/Carer Signature …….…………………….…………………………….

Date ………………………

Appendix C

Additional Advice for Parents with Internet Access at home

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.

2. Parents should agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use;

4. Parents should get to know the sites their children visit and talk to them about what they are learning;

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below);

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdfAimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
- http://www.parentscentre.gov.uk/usingcomputersandtheinternetA very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwiseIncludes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- http://www.kidsmart.org.uk/Explains the SMART rules for safe internet use and lots more besides.
- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)
- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use.