St. Patrick's & Brigid's College

E-Safety Policy

Adopted On:

Review Date:

1. INTRODUCTION

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. St Patrick's & St Brigid's 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 St Patrick's & St Brigid's College. The policy has been drawn up by the staff of the school under the leadership of Mrs D O'Kane Principal Mrs C Alexander, Head of ICT and Mr S McLaughlin, C2k Manager. It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed annually.

2. C2K

Classroom 2000 (C2k) 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 names and passwords
- Scanning all C2k 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 C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

3. 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 for Pupils (Appendix 1) and Staff (Appendix 2) containing E-Safety 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, PDAs) is subject to the same requirements as technology provided by the school.

The Head of ICT and the Principal/Senior Leadership 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

Parents/Carers consent along with that of the pupil to the ICT Code of Safe Practice for Pupils (Appendix 1) must be obtained annually before the pupil accesses the internet.

In addition, the following key measures have been adopted by St Patrick's & St Brigid's College to ensure our pupils do not access any inappropriate material:

- The school's E-Safety code of practice for use of the Internet and other digital technologies is made explicit to all pupils and E-Safety guidelines are displayed prominently in all computer rooms;
- Our Code of Practice is reviewed each school year and a signature is collected from pupils/parents to confirm that they have read and agree with it;
- 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 in Key Stage 3 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 C2K can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during school hours. During school hours pupils are forbidden to play computer games or access social networking sites.

Sanctions
Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Behaviour Policy.

Pupil use of the school network will normally be suspended whilst an investigation is taking place.

A period of suspension from the use of the network may be imposed (by the Year Head in consultation with the Head of ICT) in addition to other sanctions.

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 staff:

- Pupils accessing the Internet should be supervised by an adult at all times.
- 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.
- Teachers are aware that the C2K 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.

4. Internet Safety Awareness

In St Patrick's & St Brigid's College we believe that, alongside having a written E-Safety 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

Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, Key Stage 3 pupils are made aware and discuss Internet Safety through structured lessons. There are various pupil resources available such as:

Gridclub
Signposts to Safety (primary and secondary versions)

KidSMART
Know IT All for Schools
ThinkUKnow
Childnet's Sorted website

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 E-Safety Policy and Code of Safe Practice for Pupils (Appendix 1) is available on the school web-site. Parents/Carers must sign each year to confirm that they have read this document and give consent before their child can access the Internet in school. Additional advice/guidance for parents is contained in Appendix 3 and links to appropriate web-sites containing advice for parents with internet access at home are also posted on the school web-site.

5. Health and Safety
In St Patrick's & St Brigid's College we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite, which has 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. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are also mindful of certain medical conditions which may be effected by use of such equipment e.g. photosensitive epilepsy.

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.

6. 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. An editorial team ensure common values and quality control. 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.
- Pupils' full names will not be used anywhere on the web site, particularly in association with photographs.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7. 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. C2k 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.

Appendix 1

ICT Code of Safe Practice
Post Primary Pupils
E-Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.

- I will not download or install software on school technologies.

- I will only log on to the school network/ Learning Platform with my own user name and password.

- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.

- I will only use my school e-mail address.

- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.

- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.

- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of Mrs O'Kane, Principal.

- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.

- I will respect the privacy and ownership of others' work on-line at all times.

- I will not attempt to bypass the internet filtering system.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

Appendix 2

ICT Code of Safe Practice for Staff
E-Safety Rules

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Alexander, Head of ICT, Mr S McLaughlin, C2k Manager or Mrs D O'Kane, Principal.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.

- I will only use the approved, C2k, secure e-mail system for any school business.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.

- I will not install any hardware of software without permission of Mr S McLaughlin, C2k Manager.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school

Signature ……Date ……

Full Name ……..Job Title ……..……..

Advice for Parents:

While in school, teachers will guide pupils toward appropriate materials on the Internet. Outside school, parents or guardians bear the same responsibility for such guidance as they would normally exercise with information sources such as television, telephones, movies, radio and other media.

Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's use of Internet resources at home.

We all deserve to be able to use the internet to learn, explore and connect with each other. But all of us need to be aware of the risks involved in doing so, especially on social media. Our advice is:

- Don't share personal information or images with people you don't know.
- Don't accept friend requests with someone you don't know – not everyone online may be who they say they are.
- Set privacy settings on all devices so that only people you know can view your account.
- Don't post anything online that you are not happy to be shared, particularly nude or nearly nude images or videos. It may seem like a bit of fun with friends at the time but there is always a chance those images could be shared or get into the wrong hands and could lead to harmful situations such as stalking, abuse or blackmail.
- If someone has made you feel uncomfortable or you have had disturbing interaction online, tell police or a trusted adult. You can ring the police on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.
- The internet can be a great place but it is important to remember there are people out there who may wish to abuse, exploit, intimidate or bully you online – if this happens to you, tell someone immediately.
- Remember that if things do go wrong online, there are people who can help.
- If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further such incidents. You will not get into trouble.
- *General advice to parents:*

- The most important thing is to have conversations with your children - talk to them about the benefits and dangers of the internet so that you can empower them to use the internet safely.

- Cultivate an interest in their online activities - their favourite websites, online games and interests and keep an eye on what they are doing online.

- Don't be afraid to ask your children who they are talking to online and what they are talking about and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried because there are people who can help.

- Become a 'net-savvy' parent - the best safeguard against online dangers is being informed. Jump in and learn the basics of the Internet - read articles, take a class, and talk to other parents. You don't have to be an expert to have a handle on your child's online world.

- Go to www.getsafeonline.org for lots of useful advice and information on how to stay safe online. Safeguardingni.org will also provide information for parents and carers on e-safety.

- Other useful websites include www.thinkuknow.co.uk and www.ceop.police.uk