ONLINE SAFETY and USE OF DIGITAL DEVICES POLICY

Updated by: Mrs Ciara Cassidy and Safe Guarding Team in Term 1 2017-2018

Adopted by Board of Governors – 27th March 2018

Review Due: Term 2 2018-2019

Signature of Chairperson of Board of Governors: _____

Signature of Principal: _____

Date: _____

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 and use of mobile digital devices policy contains policies in relation to use of the internet, use of mobile digital devices and use of digital/photographic images of children. It is largely based on DENI Circular 2016/27 *"Online Safety" and DENI Circular 2016/26 "Effective Educational Uses of Mobile Digital Devices."* It should also be read in conjunction with the School's Child Protection, Positive Behaviour, Special Educational Needs and Anti-Bullying policies.

2. *E-SAFETY AND USE OF MOBILE DIGITAL DEVICES 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. Our school 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 2016/27 states that:

"We want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves."

The DENI circular 2016/26 states that:

"The pervasiveness of mobile digital devices (such as tablet computers and smart phones) in schools provides both educational opportunities (for learners and teachers alike) as well as management challenges which are different from those afforded by desktop and laptop computers."

This document sets out the policy and practices for the safe and effective use of the Internet and effective educational uses of mobile digital devices in St. Brigid's Primary School, Tirkane / Bunscoil Naomh Bríd. The policy has been drawn up by the staff of the school under the leadership of the ICT Co-ordinator and members of the Safe Guarding Team. 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**.

3. 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 of resources is safe and secure, while protecting users and systems from abuse.

When using desktops and laptops

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.

When using IPads and other mobile digital devices

Due to IPads no longer being compatible with C2K Guest Trusted, pupils and staff will use C2K Open Guest wireless. Although still managed by C2K, the filtering of C2K Open Guest is not as high as that of C2K Guest Trusted.

In C2K Open Guest:

- There is no unique login, meaning that staff and pupils have access to the same filtering policy.
- Sites categorised under the Internet Advanced Security Group (e.g. Shopping) and Internet Streaming Security Group (e.g. Youtube and BBC iPlayer) are fully available.
- Sites categorised under Internet Social Networking group are partially available (e.g. Twitter and LinkedIn are available). Facebook remains unavailable.
- All other sites blocked under C2K Guest trusted remain blocked under Open Guest
- While C2K have put in place some measures to mitigate against the risk in terms of Google and Bing search engines, there remains an element of risk of inappropriate search results being viewed. Therefore, special measures will be put in place (identified in Code of Practice) when using C2K Open Guest.

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 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, mobile digital devices and digital photographic and 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 and digital devices) are subject to the same requirements as technology provided by the school.

The ICT Co-ordinator, the Principal/Senior Leadership Team and the Board of Governors will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

A parental/carer consent letter **(Appendix 3)** accompanied by the code of practice for pupils 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 St. Brigid's Primary School, Tirkane / Bunscoil Naomh Bríd to ensure our pupils do not access any inappropriate material:

- The school's Online-Safety code of practice for Use of the Internet and other digital devices is made explicit to all pupils and Online-Safety guidelines are displayed prominently throughout the school;
- Our Code of Practice is reviewed each school year and signed by pupils/parents;
- 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 are regularly educated about online safety and online safety messages are integrated across the curriculum for pupils in all Key Stages.

When using C2K Open Guest on mobile digital devices:

- Pupils will only use the devices for set tasks during lessons. The devices will not be available to them during play times.
- When using I pads, pupils will use QR codes (when available) to access internet sites for images and research.

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

During school hours pupils are forbidden to play computer games or access social networking sites such as Facebook, Twitter etc.

Use of Mobile Phones and other digital devices

It is school policy to prohibit the use by pupils of mobile phones or other digital devices while on our school premises, grounds or on day trips or activities e.g. school swimming.

1. St. Brigid's Primary School, Tirkane / Bunscoil Naomh Bríd advises all parents/carers that pupils are not permitted to bring mobile phones and other digital devices to school on the grounds that they are valuable and may be damaged, lost or stolen. School staff can accept no responsibility for equipment which is lost, damaged or stolen in school whilst in the possession of any pupil.

2. If a pupil is found by a member of staff to be using a mobile phone or other digital device for any purpose, the device will be confiscated from the pupil and must be collected by the parent.

3. Inappropriate use of mobile phones or other digital devices will be regarded as a breach of discipline and will invoke the School's Disciplinary Procedures.

3. Pupils and parents are reminded that in cases of an emergency, the school landline telephone number **028 79643346** remains the appropriate point of contact.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Behaviour Policy. Minor incidents will be dealt with by the class teacher, more serious incidents will be dealt with by the ICT Coordinator or Principal and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's child protection policy.

Code of Practice for Staff

Staff have agreed to the following Code of Safe Practice.

- Where possible, pupils accessing the Internet and using digital devices 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 and digital devices. These are displayed in classrooms and discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- Deliberate or accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinator.
- In the interests of system security, staff passwords should only be shared with the network manager.
- 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 always be taken with a school camera or school device and images should be stored on a centralised area on the school network, accessible only to teaching staff, classroom assistants or under supervision for pupil work. (see Digital/Photographic Images Policy)
- Staff should not use their personal digital devices in class. Mobile phones should be on silent mode, stored out of sight from pupils and only used out of teaching hours.
- School systems may not be used for unauthorised commercial transactions.

5. Online-Safety Awareness

In St. Brigid's Primary School, Tirkane / Bunscoil Naomh Bríd 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 important for staff, parents and pupils.

Online-Safety Awareness for pupils

Rules for the Acceptable Use of the Internet and digital devices are discussed with all pupils and are prominently displayed in classrooms. In addition to this, pupils are made aware of Internet Safety through structured lessons

during Internet Safety Day and also by visits from outside agencies. There are various pupil resources available such as:

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

External agencies such as NSPCC may be invited in to promote internet safety for pupils.

Online-Safety Awareness for staff

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and attends regular courses. This training is disseminated to all teaching staff, classroom assistants and supervisory assistants as required.

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 Online-Safety and use of digital devices policy is made available to parents and the Pupil Code of Conduct is sent home at the start of each school year for parental signature. Additional advice for parents with internet access at home also accompanies this letter **(Appendix 4).**

6. Health and Safety

In St. Brigid's Primary School, Tirkane / Bunscoil Naomh Bríd we have attempted, in so far as possible, to ensure a safe working environment for pupils and staff using ICT resources, both in classrooms and in shared areas, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards are being used. Guidance is also issued to pupils in relation to the safe use of computers, digital devices and interactive whiteboards.

7. School Web Site

The school web site is used to celebrate pupils' work, promote the school and provide information. Staff will ensure that the website 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 and group photos are used where possible with general labels and captions.
- 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 in association with photographs.
- The Principal/ICT Coordinator 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.
- All content included on the website is edited for accuracy and suitability in English and Irish

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. Examples of social software used in St. Brigid's Primary School / Bunscoil Naomh Bríd are Fronter, Collaborate, Scratch and Microsoft Office 365.

The majority of activity in these on-line social sites usually causes no concern. When using desktops and laptops, C2k filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Careful monitoring needs to take place when pupils are using C2K Open Guest on mobile digital devices in order to ensure

that inappropriate social networking sites are not accessed. 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.
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.

Points for Children to Consider:

Follow these SMART TIPS

Safe – Never give your personal information online! Keep your name, address, mobile phone number and password private – it's like giving out the keys to your home.

Meeting someone you have met online can be dangerous. Only do so with your parents' or carers' permission and only when they are present.

Accept – Never open files, pictures or texts from people you don't know. They may contain viruses or nasty messages.

Reliable – information on the internet may not be true. Always check what you have read with an adult.

Tell your parent or carer if someone or something makes you feel uncomfortable, or if you or someone else is being bullied online or by text.

SMART TIPS based on "Helping your parents be cool about the internet," produced by Northern Area Child Protection Committee.

Appendix 1

ICT Code of Safe Practice

e-Safety and use of mobile digital devices rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will access the school C2k system with my login and password, which I will keep secret.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will ask permission from a member of staff before using the internet
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not bring my mobile phone or other personal digital devices into school
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

Appendix 2

ICT Code of Safe Practice for Staff
e-Safety and use of digital devices 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 the school Online-Safety coordinator or the 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 the ICT Coordinator/principal
- 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 only be taken using school digital devices and will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I will keep my mobile phone on silent mode and out of sight of pupils, only using it during break times or after teaching hours.

- 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 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 …….. (printed) Job Title . . . . . .

Appendix 3

Parental Agreement/Consent Letter

Dear Parent/ Carer

As part of Information and Communications Technology programme we offer pupils supervised access to a *filtered* Internet service provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However, in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the ICT Co-ordinator or Principal.

✂----------

Parent/ carer signature

We have discussed this and …….....(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at St. Brigid's Primary School Trkane / Bunscoil Naomh Bríd.

Parent/ Carer Signature …….

Date ……

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; Know the **SMART TIPS.**

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.pdf Aimed 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/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwise Includes 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.