Acceptable Use of the Internet and Digital Technologies Policy

Revised by: K Baldrick
Date: November 2019

Date:	Policy reviewed:	Policy amended:
November 2021		
November 2023		
November 2025		

This policy is based on and complies with DENI Circular Circular 2011/22 - Internet safety.

1. Introduction

In Newbuildings PS we believe that 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. This 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 above circular states that:

"A school's paramount consideration should always be the safety of pupils and staff."

This document sets out the policy and practices for the safe and effective use of the Internet in Newbuildings Primary school. The policy has been drawn up by the staff of the school under the leadership of the Principal/ICT Co-ordinator.

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 usernames and passwords
- Tracking and recording all online activity using the unique usernames and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses Filters access to web sites
- Providing appropriate curriculum software.

3.Codes 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 children

(Appendix 1) and staff (Appendix 2) 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, iPads and tablets, 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 iPads/tablets, laptops, mobile phones, camera phones, PDAs) is subject to the same requirements as technology provided by the school.

The ICT Co-ordinator will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Practice for pupils

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission will be sought from parents on an annual basis before pupils access the Internet.

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

The school's Code of Practice for use of the Internet and other digital technologies (enclosed) is made explicit to all pupils.
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 in Key Stage 2 are educated in the safe and effective use of the Internet, through several selected programmes. (See below)

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.

During school hours pupils are forbidden to play computer games or access social networking sites, unless specifically assigned by the teacher.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's discipline policy. Minor incidents will be dealt with by the Principal/ICT Co-ordinator and may result in a temporary or permanent ban on Internet use.
Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

Code of practice for staff

Staff have agreed to the following Code of Safe Practice:

Pupils accessing the Internet should be always supervised by an adult.
All pupils are 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.
Recommended websites for each year group are available under Favourites. Any additional websites used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age appropriate.
Deliberate/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, 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.
School systems may not be used for unauthorised commercial transactions.

3. Internet Safety Awareness

In Newbuildings PS we believe that, alongside having a written 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

Rules for the Acceptable use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, Key Stage 2 pupils follow a

structured programme of Internet Safety Awareness using a range of online resources.

Internet 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 then disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis.

Internet Safety Awareness for parents
The Internet Safety Policy and Code of practice for pupils is sent home at the start of each school year for parental signature. Internet safety leaflets for parents and carers will also be sent home. We will hold ICT evenings for parents when Internet safety is one of the issues addressed.

Community Use of School ICT Resources
The school's ICT facilities might be used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by C2K. They must also agree to the school's Acceptable Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

4. Health and Safety

Newbuildings PS have attempted, on 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 always supervised when Interactive Whiteboards and Digital Projectors are being used.

5. Digital and Video Images of Pupils

Parental permission is sought at the start of each school year to cover the use of photographs of pupils on the school website, in the local press and for displays etc. within school and written permission must be obtained from parent/carer.

6. School Website

Our 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 must 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.

Storage of images

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network, accessible only to teaching staff. Photographs of pupils are removed when they leave the school.

7. School iPads and BYOD (Bring your own device)

At Newbuildings PS we recognise that more and more pupils and staff have devices such as laptops and tablets. There is a facility within the school after the transformation (computer system update) that allows all devices to be connected to the school internet. Termed 'bring your own device' (BYOD) effectively this means devices such as laptops, phones and tablets owned by staff or pupils could be configured to access the school internet. This facility can only be granted when authorised by the Principal and the ICT Coordinator. This will be granted very rarely, as the school can't be sure devices brought into school are not infected with viruses etc. Likewise, users who request that their own devices are granted access to the school system, cannot be guaranteed by Newbuildings PS or C2K, that their devices will not pick up any viruses etc. Any user given permission to access the school internet will do so at their own risk.

iPads

Newbuildings PS has recently invested heavily within iPad technology. Most of these iPads were purchased through Extended Schools for the purpose of raising standards in Literacy (especially by boys) within Primary 7. As such these iPads may be given to the children to take home to help with their education. Under no circumstances should the children take photographs or videos using these iPads unless the class teacher has given them permission to use this tool. When a homework or task is set that requires the children to use the camera tool the parents will be notified that permission has been granted to do this. If using the camera, the children must ask

permission from anyone they intend to take a photograph or image from. Images taken might be used as a project within the class, so it is vital that anyone who has their image taken is aware of this. It is the responsibility of the parents/guardians to ensure that no inappropriate images are taken.

Internet

Under no circumstances should iPads taken home be used to access the internet unless permission has been granted by the class teacher. If a homework or task is set that requires the children to access the internet, then the class teacher will notify the parents/guardians. If permission is granted by the class teacher to access the internet, the children will be provided with recommended web addresses. Social media should not be accessed on the iPads. Inappropriate images or websites must not be viewed on the iPads. If a child views a website that is deemed inappropriate, they will either receive a warning from the Principal or ICT Coordinator, receive a ban for having access to the iPads for a period or in an extreme case be banned completely from accessing the iPads. Parents/Guardians will be informed of any sanctions that have been given out due to inappropriate use of the iPads.

Care of iPads

The school has insurance for the iPads it has purchased. This covers accidental damage only. If an iPad is dropped or damaged in anyway, the parents/guardians should notify school as soon as possible. The iPads will be transported to and from school by the children. When taken home the children should use the iPads responsibly. If the devices are taken outside the home (when not returning them to school) then parents/guardians will be responsible for them if they are lost or stolen. The children are given the iPads home with the understanding that they will look after them and that only they will use the devices.

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.

Most of the activities on these on-line social sites usually cause 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.

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 for Pupils (eSafety 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 emailing.

I will only open e-mail attachments from people I know, or who my teacher has approved.

I will not tell other people my ICT passwords.

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 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 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 eSafety.

Appendix 2 ICT Code of Safe Practice for Staff (eSafety 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 always adhere to its contents. Any concerns or clarification should be discussed with the ICT 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 authorized 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 IT Coordinator or 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 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 ……

Appendix 3

Sample Posters

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

B. Stoneham & J. Barrett

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Appendix 4

Principles for Internet Use ----- Children's Version

Be **SMART** Online

S	**Secret** Never give your address, telephone number, username, or password when on-line.
M	**Meeting** someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher.
A	**Accepting** e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.
R	**Remember** no offensive language, text or pictures are to be displayed, sent, copied, or received.
T	**Tell** your parent, teacher, or trusted adult if someone or something makes you uncomfortable.

Appendix 5

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school

SMILE and stay safe.

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher, or trusted adult know if you ever feel worried, uncomfortable, or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos, and anything from someone you do not know, or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix 6

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.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)
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/ The NSPCC website with online safety advice and help.
- https://www.net-aware.org.uk/ A website with help on social networks, apps and games.
- https://nationalonlinesafety.com/ A whole school community approach to e-safety with comprehensive training and resources for teachers, parents and children.