Harmony Hill Primary School

Safer Internet Policy

2024-2026

CONTENTS

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.

Safer Internet 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 Harmony Hill PS. The policy has been drawn up by the staff of the school under the leadership of the ICT Co-ordinator and principal. 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.

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 C2K Managed Desktops and Laptops

Some of these safety services include:
- Providing all users with a unique username and password
- 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.

When using iPads and Chromebooks

School iPads and Chromebooks use C2K Wireless.

In C2K Wireless:
- 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. X (Twitter) and LinkedIn are available). Facebook remains unavailable.
- All other sites blocked under C2K Guest trusted remain blocked under C2K Wireless
- 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.

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. School has 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-ordinators, 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 form (Appendix 3) accompanied by the code of practice for pupils is sent out to parents/carers upon their child's admission to the school. This consent must be obtained before the pupil accesses the internet.

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

- The school's Safer Internet Code of Practice for use of the Internet and other digital devices is made explicit to all pupils and guidelines are displayed prominently throughout the school;
- Pupils using the Internet will be working in highly visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised;
- Pupils will 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 Wireless 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 iPad, 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.

USE OF MOBILE PHONES AND OTHER DIGITAL DEVICES

SMART Watches

PUPILS ARE NOT PERMITTED TO HAVE SMART WATCHES IN SCHOOL

Smart watches that are internet and camera enabled, have the capacity to record and store voice notes or to communicate through Bluetooth or Wi-Fi, pose significant potential concerns in terms of safeguarding. Pupils are allowed to wear analogue or simple digital watches only. Pupils are not permitted to wear their smart watch on school premises at any time on the school grounds, will have it confiscated and parents may be required to collect the device at the end of the school day. Pupils who are found using their phone in school (or wearing a smart watch) will have it confiscated and parents will be required to come into school to collect the device(s).

PUPILS ARE NOT PERMITTED TO HAVE MOBILE PHONES IN SCHOOL, UNLESS AN APPLICATION FORM IS COMPLETED AND APPROVED BY THE SAFEGUARDING TEAM

- If this is approved, the phone will be kept in a safe place throughout the day, with the pupil being responsible for collecting it at the end of the school day.
- The phone must not be switched on within the school grounds.
- Harmony Hill Primary School accepts no responsibility for the safety of phones/devices that are brought into school and hereby expects all pupils who do, to be aware of the policy set out below.

[Further information is available within our Digital Device Policy for Pupils]

Pupils and parents are reminded that in cases of an emergency, the school landline telephone number remains the only 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.

Persistent or serious incidents 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 and Positive Behaviour & Assertive Discipline polices.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff: 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.**
- ° **Staff should not use their personal digital devices in class**. **Mobile phones should be on 'silent mode' and out of sight of pupils, only being used during break times or after teaching hours.**
- ° School systems may not be used for unauthorised commercial transactions.

E-Safety Awareness (Internet Safety)

In Harmony Hill PS, we believe that, alongside having a written Safer Internet 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.

E-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

Safer Schools NI

360° Safe

Whole School Digital Safeguarding Scheme P1-P7

External agencies such as Rapid, Dry Arch, NSPCC, Nexus and PSNI may be invited in to promote internet safety for pupils.

E-Safety Awareness for staff

The ICT Co-ordinators keep staff informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.

Community Use of School ICT Resources

In the event of the school's ICT facilities being used as a community resource, users are issued with separate usernames and passwords by C2K. 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.

Health and Safety

In Harmony Hill PS 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 and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, digital devices, 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.

School Website

- The school website is used to promote the school and provide information.
- Website photographs that include pupils will be selected carefully. Parents/carers are given the opportunity to decline or grant permission for the use of their child's image. This information is gathered through the Acceptable Use Agreement for ICT Systems Form completed at the point of admission
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

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 Harmony Hill PS are, Scratch, Microsoft Office 365, G Suite, Minecraft and Schoology.

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 Positive Behaviour and Assertive Discipline policy and child protection procedures.

Pupils are aware that any misuse of mobile phones/websites/email/apps should be reported to a member of staff immediately.

In accordance with the views of all schools listed on the document below, we expect parents to adhere to the following code of conduct:

Joint Guidance on Unhelpful Social Media Posting

We tend to forget that almost anyone can see what we are posting online and comments that may have been made in the heat of the moment can easily be copied and then shared by others, even after the original post has been deleted. As Lisburn schools, we wish to urge our school communities to work together, communicate appropriately, and remember at all times that parents/carers are representatives of their schools. Inappropriate actions on social media can impact negatively on the life and welfare of those connected with the school.

The partnership of parents and school is central to achieving the best pastoral and educational outcomes for all of our pupils.

▪ All parents have a responsibility in role-modelling effective, appropriate, and safe communication on social media.

▪ Parents/Guardians should be aware of their responsibilities regarding their use of social networking by accessing their own school's social media policy.

Methods of proper school communication with parents/carers include:

▪ School prospectus, school website, newsletters, texting service, emails, letters and face to face meetings.

▪ Pictures taken of pupils within the school setting/at school events should not be posted on social networking sites without other parents' permission.

▪ Parents should be aware that primary aged children should not be on social media platforms as most of these have an age restriction of 14+. It is the parents' duty to protect their children from unhelpful social media contact. It is also not the school's responsibility to deal with any social media issues which have taken place outside of school.

▪ Parents should not share complaints about a child, teacher, or school, through social media (including Parents' WhatsApp Groups) as such action, and subsequent comments by others, may cause significant emotional distress to those persons named and the school community as a whole. Every school has a published Complaints' Procedure which should be adhered to by both parents and the school.

▪ Online learning platforms used by schools, such as Seesaw and Google Classroom, should not be used by parents to share complaints as any comments made will be visible to pupils within school.

Please remember that perceived complaints written in the heat of the moment and posted on social media may have a personal bias and not necessarily reflect the whole truth about a situation or incident to viewers. We therefore advise parents not to be drawn into liking or commenting on such posts if they see them on social media.

Complaints regarding in-school incidents, should they arise, should be pursued through the appropriate channels by:

▪ Making contact with the class teacher, the Vice-Principal, or the Principal.

▪ A meeting can then be arranged at a mutually convenient time to attempt to resolve the issue.

▪ All schools have a complaints procedure that should be followed.

Parents/carers should also be aware that defamatory/unhelpful comments made online will naturally be viewed negatively by the school as the parent/carer has chosen to disregard the school's Complaints Policy. The parent will be asked to come in to speak to Senior Leadership about this breach in policy and the matter dealt with face

to face, which would have been the preferred method of dealing with the initial complaint.

THANK YOU TO ALL OUR PARENTS WHO PARTNER WITH US.

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 own unique c2k username to access the school system and associated learning resources, including Accelerated Reader, Google Workplace and Office 365 Learning Environments.

- 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 not edit, amend of misuse images stored within shared devices (such iPads or Chromebooks)

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

- I will follow the rules for mobile phones and smart watches set by 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 e-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.
- School business (including pupil names and their personal information (including, but not limited to their learning profiles)) will only be discussed within authorised Apps such as Google Workplace and Office365.
- **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 are 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 (including social media profiles), 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 (linked to Google Form)

Parent/Carer Acceptable Use Agreement for ICT Systems within Harmony Hill Primary School
Dear Parent/ Carer

Digital technologies have become integral to the lives of children and children, both within schools and outside school. These technologies provide powerful tools which open up new opportunities for everyone. They can stimulate discussion, promote creativity and enhance awareness of context to promote effective learning. Children within educational settings should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that children will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of children with regard to their on-line behaviour.

Harmony Hill Primary School will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form so that parents/carers will be aware of the school's expectations of pupils in relation to digital technologies.

To access the Google Form, click here

Appendix 4 - 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.

9. Before giving permission for their child to download an App to their device, parents should check the age rating. This is located next to the App in the devices respective 'App Store'. We would also recommend that parents should check the content as rated and reviewed by Common Sense Media before downloading the software.

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)
- https://www.commonsensemedia.org rates movies, TV shows, podcasts, books, and more so families can feel good about the entertainment choices they make for their children.

Appendix 5 - ICT Code of Safe Practice – Foundation Stage
E-Safety and use of mobile devices

- I will use the iPads or computer for tasks my teacher asks me to do.

- I will use my 4-digit code on the computers.

- I will not tell other people my 4-digit code.

- I will use kind words if I talk about other peoples' work.

- I will not search for anything unkind. If I do this by accident I will tell my teacher or classroom assistant.

- I will follow the instructions my teacher gives me when in the ICT suite.

- I know my teacher can check what I have been doing on the computer and iPad. They can tell my parent/carer if they think I have been unsafe.