



Learning together,
building for the future

Acceptable Use of the Internet & Digital Technologies Policy

Policy Review

Date agreed: April 2021

Next Review Date: September 2023

Signed by Chair of Governors:

Date: _____

Acceptable Use of the Internet and Digital Technologies Policy

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools

Introduction

At Kirkistown 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:

"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 at Kirkistown Primary School. The policy has been drawn up by the staff of the school under the leadership of the Principal.

It has been approved by governors and circulated to all parents via the school website.

The policy and its implementation will be reviewed regularly.

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. The Online Safety Code of Practice for pupils for Kirkistown Primary School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not. The scope of the Code covers fixed and mobile Internet; school PCs, laptops, ipads 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) are subject to the same requirements as technology provided by the school.

School staff will monitor the effectiveness of the Code of Practice, particularly in the light of any new developments in technology.

Online Safety Code of Practice for pupils

Pupil access to the Internet is through a filtered service, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. All pupils and parents sign a user agreement which outlines the school's expectations related to acceptable use of the internet.

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

- The school's Acceptable Use Agreement for use of the Internet and other digital technologies is made explicit to all pupils and is displayed prominently;
- Our policies are reviewed regularly and signed by pupils/parents;
- 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, where possible, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils should never use ipads or the internet during wet play times unless a task is specifically assigned by a teacher.
- Pupils in all classes will take part in appropriate and progressive lessons relating to online safety and the development of responsible digital citizens.

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.

The use of mobile phones by pupils is not normally permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff. Any pupil bringing a mobile phone to school must declare this and give it to a member of staff to be locked in the office for safe keeping for the duration of the school day.

Pupils are only permitted to play computer games during school hours that are specifically assigned by the teacher.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Positive Behaviour Policy. Minor incidents will be dealt with by the 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 school child protection procedures.

Code of practice for staff

Staff have agreed to the following Code of Safe Practice:

(see Acceptable Use Agreement for Staff)

- Pupils accessing the Internet should supervised by an adult at all times.
- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in the ICT area and are discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- 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 teacher leader.
- 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. Where photographs, *by arrangement with the Principal*, are taken on a personal device, they will be removed from these devices as soon as possible.

Internet Safety Awareness

At Kirkistown PS we believe that, alongside having an acceptable use 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 the ICT area. In addition, all 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 courses where available. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants.

Internet Safety Awareness for parents

The Acceptable Use of the Internet & Digital Technologies Policy is made available on the website and the Online Safety Code of practice for pupils is sent home for parental signature. Internet safety leaflets for parents and carers also made available via the school website and newsletters. Parents are invited to attend class assemblies and relevant information sessions.

Health and Safety

Kirkistown PS have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used.

Digital and Video Images of Pupils

Parental permission is sought 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.

Storage of images

Digital and video images of pupils are, *where possible*, taken with school equipment. Where photographs, *by arrangement with the Principal*, are taken on a personal device, they will be removed from these devices as soon as possible.

Social Software

Chatrooms, blogs and other social networking sites are blocked by the C2K filters so pupils do not have access to them in the school environment. However, 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 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.

Through the use of C2K managed forums and exchange programmes such as Fronter and Collaborate, pupils have opportunities to interact online in a safe and supported environment.

Parental agreement

Having read the school's Internet Acceptable Use Policy parents are asked to discuss the guidelines with your child and return the completed permission form and user agreement (Attached Appendix). This will be given to all new pupils upon entry to the school.

Keeping Safe During Remote Learning Online Learning Platforms – Google Classroom, Seesaw, Timestables Rockstars and Pearson Bug Club

- Google Classroom, Seesaw, Timestables Rockstars and Pearson Bug Club are currently the online platforms being used by teachers in Kirkistown Primary School to provide resources for students remotely and mark work submitted online. Other online platforms may be trialled or employed to enhance online learning and parents will be informed of any such changes in due course.
- Children will not be expected to sign up to anything with a personal email address. They will either be provided with a school email address or a username and password.
- Parents should ensure that their child always keeps their login to this facility private and that they do not share their account with anyone. This includes any other friends.
- Some online learning platforms include a chat function or message boards, etc. It is important that parents monitor the use of these facilities and that children understand what is appropriate to write online. Parents should remind their children that these messages will be visible to the school staff and they should not put anything in a message, that they would not want anyone else to see. Our school has the same expectations of behaviour online as it does when pupils are physically in school.
- Do not put unnecessary personal information in the user profile of these apps. For example, try to keep location, phone number and dates of birth private.
- Always check the terms and conditions of the programs, especially those around age. For example, by default, Skype restricts the privacy settings of users under 16 years old. However, in Kirkistown Primary School we will be using online platforms specifically designed for children.
- Help to educate your child on how to use online learning programs to ensure they are safe. Careless use of other platforms or underage use of social media can lead to a breach of personal security, downloading viruses or malware or

even contact from people who the children do not know and may have malevolent intent.

- Children should never accept instant messages, phone calls, screen sharing or files from anyone they do not know and parents should reinforce and monitor this.

Video Conferencing

- From time-to-time teachers may decide to deliver online learning using videoconferencing programs such as Google Meet. These programs enable students to talk to each other, and potentially their teacher. Whilst they are a great way to keep in touch, to safeguard both students and staff, one-to-one tuition will not normally take place using video conferencing unless by prior arrangement with a parent and with the knowledge and approval of the Principal. A teacher may, however, record a video to provide additional support to a particular child or group of children with their learning. Where video conferencing is used, parents will be provided with a clear list of instructions on how to access and use the service alongside simple expectations around the use of such technology.

Protecting the Home Network

- It is important that parents make sure that their home Internet network is secure. Increased use of the Internet for anything increases the risk of clicking on or downloading something nasty to your network, so it's important that parents have anti-virus / anti-malware software installed to ensure the safety of everyone in the family.
- Keep all anti-virus program updated regularly. There are new attacks every day and the amount of malicious content on web applications is rapidly increasing in both frequency and expertise so it is important to always stay up to date.
- If parents have a wireless router, they should check that the wireless network is secure so that people living nearby cannot access it. It is best to set up a home network so only people with a wireless 'key' (i.e. password) can connect to it.
- If a network is secure, users will be prompted for a password when they try to access it for the first time and there should be a padlock symbol next to the network name. If this does not happen, the network is not protected and anyone will be able to join.
- It is always best to change the name of a home network – but not to anything that identifies the family. Parents should also change the default password, as these are often freely available to attackers online if they know where to look. Parents should choose a password of at least 8 characters, with a mix of case,

numbers and symbols. The current advice is to pick three random words or a memorable phrase.

- Parents should always cross-check any information if they are not sure about what their child is being asked to do. If in any doubt, parents should make contact with the class teacher or the school.
- Further information on keeping safe while using popular apps is available from the Kirkistown Primary School website:

<http://www.kirkistownprimaryschool.com/staying-safe-online.html>

Addendum

Due to COVID-19 the pressures on children and their families are significant. There will be heightened awareness of family pressures through being contained in a small area, poverty and financial or health anxiety. This may have an impact on the mental health of both parents and children and the resulting behaviour. Should any member of staff be concerned about the behaviours of any child / family or should a child or family member contact them by Seesaw / Google Classroom and make a disclosure, they must contact the Principal and Designated Teacher without delay, detailing the nature of their concerns and any relevant information regarding any potential disclosure. An informal 'Report of Concern' should be completed at the nearest opportunity and, should a disclosure be made, a formal 'Note of Concern' completed.

Network administrators reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibly – they will respect the right to privacy whenever possible

Any parent or member of staff who wishes to discuss this document can put any questions to:-

Mr Graham (Principal)

This document is based on

Acceptable Use of the Internet and Digital Technologies in Schools

(DENI Circular 2007/1 and 2016/27)

THIS POLICY WILL BE REVIEWED IN 2023.



Learning together,
building for the future

Online Safety Code of Practice for pupils

At Kirkistown Primary School, you are encouraged to use Information Communication Technology (ICT) to help enhance your learning. This technology must be used in a responsible way, ensuring you do not put yourself or others at risk when at home or in school.

For my own safety:

- I understand that school will monitor how I use ICT Systems
- I will tell an adult if I see or hear any unpleasant, unkind or inappropriate material or messages

For my own learning and the learning of others:

- I will respect the work and property of others and not copy, remove or change someone else's files or work
- I will use search engines, apps and websites appropriately, as directed by the task set by my teacher
- I will take care while using the school's ICT equipment to prevent it being damaged
- I will be polite and responsible when communicating with others
- To be environmentally friendly, I will only use the printer when I have checked my work and have got permission from the teacher to do so

I understand that I am responsible for my actions inside and outside of school:

- I understand that I may lose access to the school network if I am unable to follow the requirements of the Acceptable Use and Online Safety Code of Practice for pupils
- I will not take or send images of ANYONE without their permission or post photos of pupils on any social networking sites
- The school may be obliged to report my or the actions of others to the police if a young person's safety is at risk

Signed (Pupil) _____ Signed (Parent/Carer) _____

Date _____