E-Safety Policy

Earlview Primary School and Nursery — Watch your children grow...

Agree Date	Review Date	Persons Responsible	Designated Governor
March 2024	March 2025	Mr. Smith	Rev. Keaveney

Context

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circular 2011/22 and 2013/25 on Internet/E-Safety. This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Earlview Primary School and Nursery. It also links to Article 17 from the UN Convention on the Rights of the Child which states:

"You have the right to get information that is important to your well- being, from radio, newspaper, books, computers and other sources. Adults should make sure the information you are getting is not harmful, and help you find and understand the information you need."

Care and responsibility

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. With these opportunities we also have to recognise the risks associated with the internet and related technologies.

The use of these exciting and innovative tools in schools and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information. ␣SEP␣
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.

- Plagiarism and copyright infringement
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person as with all other risks, it is impossible to eliminate the risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise.

In Earlview Primary School and Nursery we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach pupils appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

As E-Safety is an important aspect of Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the E-Safety Co-ordinator (Mr. Smith) and the E-Safety Team including ICT Co-ordinator to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. This team has the responsibility for leading and monitoring the implementation of E-Safety throughout the school. The E-Safety Co-Coordinator/Principal has the responsibility to update Senior Management and Governors with regard to E-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

E-Safety Skills Development for Staff

- All staff will receive regular information and training on E-Safety issues through the Co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E- Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons.
- New staff members will receive a copy of the E-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.

Handling of E-Safety Issues

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Co-Coordinator to be recorded in the E-Safety log. Issues of a child protection nature will be reported to the designated teacher and dealt with in accordance with the Earlview Primary School and Nursery Child Protection and Safeguarding Policy. Incidents of pupil misuse of technology which arise will be dealt with in accordance with the Earlview Primary School and Nursery Positive Behaviour Policy. A record of very serious incidents will be recorded on the Private folder on the school network.

E-Safety and Pupils

E-safety will be discussed with pupils at the start of the year when they receive their Acceptable Use Agreement. This should be discussed as a set of rules that will keep everyone safe when using technology in school. It will also be discussed as they accept the agreement through their My School log in. Activities throughout the school year including visits from the PSNI will refresh E-Safety and further pupils' understanding.

Securus e-safety tool

Earlview Primary School and Nursery have implemented the Securus e-safety tool through the C2K network. This tool aims to safeguard children in their use of information systems and electronic communications. The tool monitors the screen display and keystrokes of pupils on C2K managed machines and triggers a capture if the content is listed in the database of inappropriate words and phrases. These reports are accessed by the school principal and other appointed senior teachers.

E-Safety and Parents

The Earlview Primary School and Nursery E-Safety policy will be published on the school website and parents will be encouraged to read the document. Parents will be required to read the Acceptable Use Agreement for pupils and sign this agreement following discussion with their child.

Earlview Primary School and Nursery will look to promote E-Safety awareness within the school community which may take the form of parents' information sessions, information leaflets or links on the school website.

Safer Schools NI App

We are registered with Safer Schools NI. This app is designed to help navigate the digital world that our children and young people live in every day. It will help by giving you the tools to protect the children and young people in your care online.

E-Safety and Staff

All staff will be introduced to the E-Safety policy and its importance explained. Staff will be asked to read and sign the Acceptable Use Agreement for Staff which focuses on E-Safety responsibilities in accordance with the Code of Conduct. Staff should be aware that all Internet traffic and email is monitored, recorded and tracked by the C2K system (this will continue as an aspect of security within C2K's replacement system).

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials, some of which could be unsuitable.

Networks

Pupil access to the Internet is through:

1. A filtered service provided by C2K (this will continue as an aspect of security within C2K's replacement system), which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet on admission to Earlview Primary School and Nursery.

Connection of iPads and personal devices is through the controlled C2K Guest wireless network and is subject to the same level of filtering as the main school system.

At the discretion of the principal, staff can be given enhanced internet filtering to allow for the use of You-Tube and other websites needed for educational purposes. When staff have been given enhanced filtering they must ensure that no pupil is given access to a computer that they are logged on. Staff should always ensure that any internet searches should not be carried out while connected to a projector and that any use of YouTube is only after checking the content and ensuring that children are not exposed to adverts or other

content.

Teaching and Learning Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.

- Educating pupils on the dangers of technologies that may be encountered outside of school will be discussed with pupils P4-7 on a regular basis by teachers and by the PSNI. [SEP]

- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/guardian, teacher/trusted member of staff.

- The school Internet access is filtered through the C2K managed services.

- No filtering is 100% effective; therefore all children's use of the internet is supervised by an adult.

- Use of the internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Children will be taught to be 'Internet Wise'. They will be made aware of Internet Safety Rules and encouraged to discuss how to cope if they come across inappropriate material.

E-mail

- Pupils may only use C2K e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children will not always be given individual e-mail addresses. In some instances, children may have access to a group e-mail to communicate with other children as part of a particular project.

Messages sent and received in this way will be supervised by the teacher.

School Website / Facebook (see Facebook policy)

The Earlview Primary School and Nursery website promotes and provides up to date information about the school and showcase other aspects of school life. In order to minimise risks of any images of pupils on the school website / Facebook being used inappropriately the following steps are taken:

- Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa.
- The website does not include home addresses, telephone numbers, personal e-mail or any other personal information about pupils or staff.

Social Networking

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- A definition is of cyber-bullying is provided within the Anti- Bullying policy and staff are made aware that pupils may be subject to cyber-bullying via electronic methods of communication both in and out of school.
- Our pupils are asked to report any incidents of cyber-bullying to the school. School staff will not add children as 'friends' if they use these sites.

Password Security

- Staff users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils, and should be changed if it appears pupils have worked out an adult's password.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

Mobile Phones and other electronic devices

It is important to be aware of the safety issues regarding mobile phones and other devices which now increasingly have Internet access. Pupils are not permitted to bring such devices into school. Staff use of mobile phones, only when necessary, should be discreet. Mobile phones should not be used in the classroom setting.

Acceptable Internet Use Agreement for Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's E-Safety policy has been drawn up to protect all parties – the students, the staff and the school. This policy applies to any internet access within school for staff.

The school reserves the right to examine and delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal agreeing that:

- All internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mails can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.