Reviewed October 2024

Enniskillen Model Primary School

E – Safety Policy and Acceptable use of the Internet & Digital Technologies Agreements

1. E-Safety

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and also guidance from DENI Circular 2011/22 Internet Safety, 2013/25, 2015/21, 2016/26 'Online Safety'. These provide guiding principles for keeping pupils and the wider school community safe online and for prioritising online safety within the school's preventative education curriculum and overall Safeguarding Policy. In addition to guidance and correspondence issued by the Education Minister in September 2024 re the use of Mobile Phone in schools.

Context:

This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Enniskillen Model Primary School.

It also adheres 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 information you are getting is not harmful, and help you understand the information you need.'

E-Safety is short for Electronic Safety. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions.

E-Safety covers not only internet technologies but also electronic communication via mobile phones, game consoles and wireless technology as well as collaboration tools and personal publishing.

E-Safety in School:

• Is concerned with safeguarding children and young people in the digital world

• Emphasises learning to understand and use technologies in a positive way

• Is less about restriction – instead focusing on educating about the risks as well as the benefits so that users feel confident online

• Is concerned with supporting pupils to develop safer online behaviour both in and out of school

• Is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately

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 communication channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings children into contact with people from all sectors of society and with a wide range of materials, some of which could be unsuitable.

The rapidly changing nature of the Internet and new technologies means that e-safety is an ever growing and changing area of interest and concern.

This e-safety policy reflects this by keeping abreast of changes taking place. Schools have a duty of care to enable pupils to use on-line systems safely.

This e-safety policy operates in conjunction with other school policies:

• Positive Behaviour and Anti Bullying

• Safeguarding and Child Protection

• Acceptable Use of the Internet and Digital Technologies Agreements

E-Safety must be built into the delivery of the curriculum. Using ICT is a compulsory cross-curricular element of the NI Curriculum and schools must ensure acquisition and development of these skills by pupils.

This policy highlights the need to educate pupils about the benefits and risks of using technology and provide safeguards and awareness for users to enable them to control their online experiences.

E-Safety in Enniskillen Model Primary School depends on effective practice at a number of levels:

• Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies

• Sound implementation of E-safety policy in both administration and curriculum including a secure school network design and use

• Safe and secure Internet provision by C2K

Care and Responsibility:

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

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, they can also place users at risk within and outside school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to or loss of or sharing of personal information

• The risk of being subject to grooming by those with whom they make contact

• The sharing or distribution of personal images without an individual's consent or knowledge

• Inappropriate contact or communication with others, including strangers

• Cyber-bullying

• Access to unsuitable video or internet games

• An inability to evaluate the quality, accuracy and relevance of information

• Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on social and emotional development

As it is impossible to eliminate the risks completely it is therefore essential through good educational provision to build pupil resilience to any risks to which they may become exposed so that they have the confidence and skills to deal with any scenario which may arise.

In Enniskillen Model Primary School, we understand the responsibility to educate pupils in e-safety issues. We aim to teach pupils appropriate behaviour and critical thinking to enable them to remain safe when using the Internet and related technologies, in and outside the classroom.

Roles and Responsibilities:

As e-safety is an important aspect of safeguarding and protecting children the school's e-safety team, principal and Board of Governors have the ultimate responsibility to ensure the policy and practices are embedded and monitored. It is the role of the e-safety team (including the ICT Co-ordinator and C2K managers) 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-ordinator (Mr Rainey) and the principal (Mr Glass) have the responsibility to update the Senior Leadership Team and the Board of Governors with regard to e-safety and all governors should have an understanding of the issues relevant to the school in relation to local and national advice.

The E-Safety Co-ordinator:

• Leads the E-Safety Team (Mr Rainey, Mrs Hurst, Mrs Keys and Mr Glass)

• Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policies and documents

• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident

• Provides training and advice for staff

• Liaises with Education Authority

• Receives reports of e-safety issues and creates a log of incidents to inform future e-safety developments

• Reports regularly to the principal and SLT

• Receives appropriate training and support to fulfil the role effectively

• Has responsibility for passing on requests to C2K for the blocking/unblocking of internet sites

• Maintains an e-safety log book indicating any occasions where the school has used its powers of search and deletion of electronic devices

The Board of Governors:

• Is responsible for the approval of the policy and reviewing its effectiveness. They should receive regular information about e-safety incidents and monitoring reports.

The Principal:

• Is responsible for ensuring the safety (including e-safety) of all members of the school, though the day-to-day responsibility for e-safety is delegated to the e-safety co-ordinator.

• The Vice-Principal should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (refer to disciplinary procedures and/or Child Protection/Safeguarding Children policies).

Teaching and other Staff

• Have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices

• Have read, understood and signed the school's Acceptable Use of the Internet Policy for Staff

• Report any suspected misuse or problem to the school's e-safety coordinator

• Embed e-safety guidance into the curriculum and other school activities as appropriate.

E-Safety Skills Development for Staff:

E-Safety training is an essential of staff induction and should be part of continuous professional development. Through this policy we aim to ensure that all reasonable actions are taken and measures put in place to protect all users.

• All staff will receive regular information and training on e-safety issues through the e-safety coordinator at staff meetings

• All staff must be 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 the 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 be asked to sign an Acceptable Use of the Internet agreement

• Staff who request enhanced internet access on the C2K network will be informed of the appropriate use

Handling of E-Safety:

Issues of misuse and/or access to inappropriate material by any user should be reported as soon as possible to the e-safety coordinator (Mr Rainey) who will record the incident in the e-safety log, giving details of the time, website, etc.

Issues of a child protection nature should be reported to the designated teacher (Mrs Keys) or any other member of the Safeguarding Team who will deal with the issue in accordance with the Child Protection/Safeguarding Policy.

Incidents of pupil misuse of technology will be dealt with in accordance with the Positive Behaviour and Anti-Bullying policy. Pupils must be made aware that misuse of the Internet may lead to access being denied.

A record of serious incidents will be kept in the Safeguarding and Child Protection log book (in a locked cupboard).

The E-Safety Log Book will be made available to the, SLT, Principal, Board of Governors and E-Safety Team.

Illegal or Inappropriate Activities:

The school believes that the activities listed below are inappropriate (and on occasions illegal) within a school context and that users should not engage in these activities when using school equipment or systems (both inside and outside school). Users should not visit internet sites, make, post, upload, data transfer, communicate or pass on any material, remarks, proposals or comments that contain or relate to:

• Child sexual abuse images (Illegal – The Protection of Children Act 1978); grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)

• Possession of pornographic images (illegal – Criminal Justice and Immigration Act 2008); criminally racist material in UK; to stir up religious hatred or hatred on the grounds of sexual orientation (illegal – Public Order Act 1986)

• Promotion of any kind of discrimination

• Promotion of racial or religious hatred

• Threatening behaviour, including promotion of physical violence or mental harm

• Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally, the following activities are also considered unacceptable use of equipment provided by the school:

• Using school systems or equipment to run a business

• Use systems, equipment, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by C2K

• Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties without the necessary licensing permissions

• Revealing or publishing confidential or proprietary information (e.g. financial or personal information, databases, computer or network codes and passwords)

• Creating or propagating computer viruses or other harmful files

• Online gambling and non-educational gaming

• Use of personal social networking sites or profiles for non-educational purposes

If staff suspect misuse might have taken place but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour or disciplinary procedures.

E-Safety and Pupils:

Pupils need to know how to cope if they come across inappropriate material situations online. E-Safety will be discussed with pupils on an ongoing and regular basis. This should be discussed as a set of rules that will keep everyone safe when using technology in school. It will be discussed as they accept the My School log in agreement.

Activities throughout the year including Internet Awareness Day and possible visits from the PSNI (KS2) and NSPCC will refresh e-safety and further pupils' understanding.

Pupils in KS2 (Y6 and Y7) could also use the Cyber Café/Think U Know/Bee safe Program resources as part of their PDMU programme.

Children in Enniskillen Model Primary School are not permitted to have mobile phones in school.

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 of the Internet Agreement for Staff which focuses on e-safety responsibilities in accordance with the Staff Code of Conduct. Staff should be aware that all internet traffic (including email) is monitored, recorded and tracked by the C2K system.

At the discretion of the principal, staff can be given enhanced internet access to allow the use of websites for streaming of videos (e.g. YouTube) for educational purposes only. When staff have been given enhanced internet access they must ensure that no pupil is given access to a computer or other device.

Staff should always ensure that internet searches involving sites that have been granted enhanced access should not be carried out when children can view e.g. on a computer screen or an IWB (interactive whiteboard). The use of such sites should

only take place after the content has been checked to ensure that pupils are not exposed to inappropriate material.

Staff in Enniskillen Model Primary School are not permitted to use their own personal devices such as mobile phones during contact hours with children or using those devices as cameras to take pictures of children when in school. Staff are allowed to use their own devices in non-contact time, during times such as break and lunch.

E-Safety and Parents:

The E-Safety Policy will be published on the school website and parents will be encouraged to read the document. Enniskillen Model Primary School will look to promote e-safety awareness within the school community which may take the form of information evenings for parents/carers, information leaflets and/or links on the school website.

Information for parents is available on the Think U Know website: www.thinkuknow.co.uk

Teaching and Learning – Internet Safety:

Staff and pupils accessing the internet via the C2K network will be required to authenticate using their C2K username and password. This will provide internet filtering via the C2K Education Network.

Access to the internet via C2K is fully auditable and reports are available to the school principal.

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 in an age appropriate way on a regular basis with teachers and other agencies (e.g. PSNI project)

• 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 made aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. parent/guardian, teacher, Childline

• The school's internet access is filtered through the C2K managed service

• No filtering is 100% effective therefore all children's use of the internet in school is supervised by an adult

• Use of the internet should be a planned activity. Aimless surfing is not encouraged. Children are taught to use the internet in response to a need e.g. researching a question that arisen from work in class

• Pupils will be taught what internet use is acceptable and what is not and be 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 (Internet Safety Rules will be displayed in classes) and encouraged to discuss how to cope if they come across inappropriate material

Email Use:

• C2K recommends that all staff and pupils should be encouraged to use their school email system for school business; it is strongly recommended not to use home email accounts for school business

• The C2K filtering solution provides security and protection to C2K email accounts by offering scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content

• If pupils are given access to email in school they may only use C2K email accounts

• Pupils must immediately tell a teacher if they receive an offensive email

• Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission

• The forwarding of chain mail by staff or pupils is not permitted

• Pupils will not always be given individual email addresses. In some instances, pupils may have access to a group email to communicate as part of a school project. Messages sent and received in this way will be supervised by the teacher

School Website:

Enniskillen Model Primary School's website promotes and provides information about the school and may showcase aspects of school life. In order to minimise risks of any images of pupils on the school website the following steps are taken:

• Group photographs are used where possible with general labels/captions

• Photographs of pupils on the school website may only be published if permission has been granted by the parent/carer

• Names and images are kept separate e.g. if a pupil is named their image is not used

• The website does not include addresses, telephone numbers, personal email or any other personal information about pupils or staff

Social Networking:

Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals).

Social environments enable any community to share resources and ideas amongst users. There are many excellent public examples of social software being used to support formal and informal educational practice amongst young people and

amongst educators. They are also popular ways of enabling users to publish and share information, including photographs, video from webcams, video files and blogs about themselves and their interests.

C2k filters out services which are misused and block attempts to circumvent the filters. Pupils will not be allowed to use any social software which has not been approved by teaching staff and the C2K filtering service.

Staff and pupils are advised that it is not acceptable or school policy for them to be friends on social network sites (e.g. Facebook). Pupils in this school are told they should not request to be friends with a member of staff on a social network site. Equally, staff are also told that they must not request to be friends or accept requests to be friends with pupils or past pupils of the school on any such site. This is good practice in line with child protection/safeguarding children policy.

• The school C2K systems deny access to social networking sites.

• Pupils and their parents/carers are 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.

• Cyber-bullying is addressed within this 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. (More information provided below).

• Our pupils are asked to report any incidents of cyber-bullying to the school

Social networking through the use of Internet-based and other electronic social media tools is integrated into everyday life. Use of Facebook, Twitter, blogging, wikis and other online social media vehicles are now commonplace with the result that the lines between work and personal life can become blurred. To protect staff, pupils and the reputation of the school the following guidelines should be followed:

- Staff should not use school systems or equipment to engage in personal social activities e.g. Facebook, Twitter, blogging, wikis, etc. This inappropriate use may be treated as a disciplinary matter
- If staff use social media sites for personal use they are reminded that they have a responsibility to ensure they are posting comments or images that are not detrimental to their position as a member of staff of Enniskillen Model Primary School, the privacy or rights of other staff or pupils and the reputation of the school. A common sense approach to the use of social media sites is recommended

Mobile Technologies: Mobile Phones and other Electronic Devices (including (BYOD) Bring Your Own 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 allowed mobile phones in school. Other electronic devices which have internet access will not be allowed to be connected to the school C2K Wireless

network and children must use these devices appropriately. Children must refrain from taking pictures with these devices.

Staff members should refrain from using their mobile phones or similar technology when in contact with children unless prior permission has been given by the Principal. Under normal circumstances, mobile phones and personal electronic devices belonging to staff should not be in view of the children. Calls / texts must be made / received in private during non-contact / break times when no children are present.

If photographs of pupils are being used by staff for lessons, presentations, website etc., then they should be stored on the C2K system. Any photographs taken by a staff member and stored should be kept to to the school's C2K system. School devices such as ipads, surface pros or school cameras should be used to take photos and saved on the school network systems.

Staff should not store pupils' personal data and photographs on memory sticks unless password protected.

The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.

Access to the Internet on such non C2K devices for school related business only be granted using the C2K Wireless access and therefore is subject to C2K's filtering service.

We request that parents / guardians refrain from using their mobile phones and electronic devices in and around the school premises. Any photographs taken in school are only to be taken of their own child/children and are only for personal use. Group photographs in assemblies, sports days etc are not to be shared in the public domain through social media etc…

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Managing Remote Learning Sessions

Staff communicating with pupils and parents on Google Classroom or other online platforms such as Meet.

- Comment using appropriate language and correct use of English.
- Address pupils and parents correctly.
- Comment on the pupils work in private messages only.
- When making videos or on live chat you must be in appropriate clothing and have a neutral background (e.g. not in a bedroom). No other family member should be in the background.
- You may communicate with your pupils in the stream on Google Classroom, and whilst it may be less formal, adhere to the above rules.
- Always have another member of staff present in a live chat.

- Be available to answer questions on Google Classroom and emails between 9:00am and 3:00pm.
- Setting work at the latest, by 3pm on the day before the work is expected to be completed.

Pupils and parents communicating with staff on Google Classroom or other online platforms.

- Comment using appropriate language and correct use of English.
- Address staff members correctly e.g. Mrs/Miss/Mr/Ms
- You may ask general questions in the stream but ensure it is appropriate.
- When discussing a piece of work this should be done in a private message.
- When making videos or on live chat you must be in appropriate clothing and have a neutral background (e.g. not in a bedroom). No siblings in the background.
- Inappropriate comments will be recorded with a screen shot and sent to the Principal.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.

- Access to the Internet will be supervised.

- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.

- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

• Staff are provided with individual usernames and passwords which they are encouraged to change periodically. Login details should not be shared with pupils and should be changed should it appear pupils have worked out a staff password

• All pupils are provided with an individual username and password

• Pupils are not permitted to deliberately access files on the school area which belong to any other users

• Staff area/folders are the individual responsibility of staff to ensure and protect the security and confidentiality of the school network

Cyber Bullying:

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. Pupils engaging in cyber bullying may be dealt with in line with the school's 'Positive Behaviour Policy' and 'Anti-Bullying Policy'.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content;
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity;
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile;
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites;
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people;
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

- A record is kept of all incidents of cyber-bullying and reported to the e-Safety team. This allows the schools e-Safety team to monitor the effectiveness of the school's preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

Network Access:

Internet access for all staff and pupils is through the filtered service provided by C2K.

The C2K 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 – pupils, staff and the school.

The school reserves the right to examine and delete any files that may be held on its computer system and to monitor internet sites visited and emails sent and received.

Staff should read and sign a copy of the school's Internet Use Agreement for staff and return to the principal.

This E-safety policy and its implementation will be reviewed annually and updated.

Handling e-Safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the UICT Co-ordinator and recorded in the e-Safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints' procedure.

2. Acceptable Use of the Internet and Digital Technologies

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 Code of Safe Practice for Enniskillen Model PS makes it 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) is subject to the same requirements as technology provided by the school.

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

Filtering:

C2k provides an effective filtering system, as a result of which the following categories of websites are not, by default, available to Enniskillen Model PS:

• Adult: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;

• Violence: content containing graphically violent images, video or text;

• Hate material: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds;

• Illegal drug taking and the promotion of illegal drug use: content relating to the use or promotion of illegal drugs or misuse of prescription drugs;

• Criminal skill/activity: content relating to the promotion of criminal and other activities;

• Gambling: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

If at any time school staff or pupils find themselves able to access from within the C2k system internet sites which they think should be blocked, they should advise the school Principal (or, in his absence, his immediate deputy). The Principal should then report the matter to the C2k Helpdesk which will implement agreed procedures for handling such issues. Depending on the nature of the issue, these procedures may require C2k to report to the Department. All actions should be taken immediately. Enniskillen Model PS's paramount consideration in this matter is the safety of pupils and staff.

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 is sought from parents before pupils (from Primary 4 – 7) access the Internet.

The following key measures have also been adopted by Enniskillen P.S. 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 (Appendix 1) is made explicit to all pupils and is displayed prominently;

• 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 P4-P7 are educated in the safe and effective use of the Internet, through recommended programmes.

Sanctions:

Incidents of technology misuse which arise will be dealt with in accordance with the school's Positive Behaviour and Anti Bullying Policy. Minor incidents will be dealt with by the Principal and/or UICT Co-ordinator. This 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.

Internet Safety Awareness:

In Enniskillen Model P.S. 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.

1. **Internet Safety Awareness for pupils**

SMART rules for the Acceptable use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, Key Stage 2 will have additional activities to enhance their Internet Safety Awareness using a range of online resources and outside agencies. (see Appendix)

2. **Internet Safety Awareness for staff**

The UICT 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 as appropriate. Staff access to the internet is through a filtered service provided by C2K. All staff will agree to an acceptable use of the internet which follows the code of practice (see Appendix 2).

3. **Internet Safety Awareness for parents**

The Internet Safety Policy and Code of practice for pupils is sent home for parental signature. Internet safety leaflets for parents and carers also are sent home on a regular basis. As deemed appropriate, parents will be offered an update on E Safety through an information seminar led by the Principal, UICT Co-ordinator or a relevant external organisation.

Health and Safety:

Enniskillen Model 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 Library. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. It is made clear to all users that no one should stare directly into the beam of the projector.

Digital and Video Images of Pupils:

The developments of digital images and videos have significant benefits within the curriculum and enhance learning. Image and videos may either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils are made aware that once an image/ video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognize the risks attached to publishing their own images on the internet e.g. on social networking sites.

Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute. (see Safeguarding and Child Protection Policy Appendices/Staff Code of Conduct)

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 on the Safeguarding and Child

Protection Information Sheet on entry into school. (see Safeguarding and Child Protection Policy)

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area called ‘Staff Resources’ on the school network, accessible only to staff. In circumstances agreed beforehand with the Principal that staff use a personal device - images/videos etc must be placed on the C2K system and removed from the device as soon as possible.

Our school website provides up to date information about the school. A gallery of photographs will inform the public of aspects of school life throughout the school year. In order to minimise risks of any images of pupils on the school website 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-mails or any other personal information about pupils or staff.

• Group photos are used where possible, with general labels/captions;

• Images are ONLY used if parental permission has been obtained. (See permission form, below.)

Parental agreement:

Having read the school's Internet acceptable use policy parents are asked to complete and return a permission form and user agreement on behalf of their child. This is available from the office and will be given to all new pupils upon entry to the school in the front of their school homework diary. This particular form will be sent home for parents to sign on an annual basis.

A SUMMARY OF THIS POLICY IS IN LEAFLET FORMAT WHICH IS ON DISPLAY AND CIRCULATED TO PARENTS PERIODICALLY

MOBILE PHONES

Enniskillen Model Primary School does not advocate the use of mobile phones by children in school or on trips.

Be aware of the safety issues regarding mobile phones. Increasingly these may have Internet access.

Encourage your child / children to talk about how they use mobile phones. Remind your child / children not to give mobile numbers to strangers and people they do not know very well. Talk about responsible use of text messaging.

Points for Children to Consider

Follow These SMART TIPS

Secret – always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART TIPS from "Helping your parents be cool about the Internet", produced by: Northern Ireland Area Child Protection Committee.

School will update/alert parents on current social media 'issues' via text message/Facebook/website.

Points for Parents to Consider:

It is important to promote Internet Safety in the home and to monitor Internet use.

1. Remember that the Internet is available to your child / children in a number of devices. These could include a PC, laptop, IPad, games console and/or a mobile phone.

2. Take an interest in what children are doing. Discuss with the children what they see and why they are using the Internet.

3. Monitor on-line time and be aware of excessive hours spent on the Internet.

4. Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.

5. Discuss the fact that there are websites which are unsuitable.

6. Discuss how your child/children can respond to unsuitable material/requests.

7. Tell your child/children – Never to give personal information on the Internet.

8. Remind your child/children that people on-line may not be who they say.

9. Be vigilant. Ensure that your child/children do not arrange to meet someone in person, that they may have met on line.

10. Be aware that your child/children may be using the Internet in places other than in their own home or at school.

11. Remember that if your child/children own a “smart” phone, they have access to the Internet 24 hours a day – possibly many of those hours whilst out of your sight!

12. Rules for the Internet must apply just as much on a mobile phone as on a computer.

Please note that signing into Social media platforms e.g. Facebook, snapchat, Tic Tok legally requires your child to be 13 years old.

Reviewed October 2024

Acceptable Use for Pupils

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only.
- I will only send e-mail / messages which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
- I will not intentionally cause damage on or to the computer system, or waste resources.
- I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/cares will be informed.

Reviewed October 2024

Enniskillen Model Primary School

Rules for Responsible Internet Use
Foundation Stage

The school has installed computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will listen to what my teacher asks me to do and use the computer sensibly.

PUPIL signature: _____ Date _____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the school computers. I have read the above stated rules for use of the school computer, iPad, school network and Internet and accept responsibility for setting and conveying appropriate standards for my child.

Parent/Guardian signature: _____ Date: _____

Print name of pupil: _____ Class: _____

Reviewed October 2024

Enniskillen Model Primary School

Rules for Responsible Internet Use Key Stage 1

The school has installed computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will use my own login username and password.
- I will not open, change or delete anything without asking.
- I will not download any software or apps.
- I will not open other people's files or change their work.
- I will only use the computers for school work and homework.
- I will ask before using the Internet.
- I will not give my home address or telephone number.
- I will not give out names, addresses, phone numbers or photographs.
- I will tell a teacher if I see anything I am unhappy with.
- I will make sure my comments on Google classroom are polite and sensible.
- I understand that the school may check what I do on the computer.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet and/ or the school computers and iPads.

PUPIL signature: _____ Date _____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the school computers. I have read the above stated rules for use of the school computer, iPad, school network and Internet and accept responsibility for setting and conveying appropriate standards for my child.

Parent/Guardian signature: _____ Date: _____

Print name of pupil: _____ Class: _____

Reviewed October 2024

Enniskillen Model Primary School

Rules for Responsible Internet Use Key Stage 2

The school has installed computers, iPads and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will not bring USB devices into school unless I have been given permission.
- I will ask permission from a member of staff before using the internet.
- I will use the Internet for research and school purposes only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and sensible
- I will make sure my comments on google classroom are polite and sensible.
- I will not give my name, address or phone number or arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will respect the privacy of others. I will not give out names, address, phone numbers or photographs.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that I store files and documents, that are password protected, on Google Drive that I can access through the teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I understand that if I deliberately break these rules I may not be allowed to use the Internet and/or the computers and iPads.

PUPIL signature: _____ Date _____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the school computers. I have read the above stated rules for use of the school computer, iPad, school network and Internet and accept responsibility for setting and conveying appropriate standards for my child.

Parent/Guardian signature: _____ Date: _____

Print name of pupil: _____ Class: _____

Enniskillen Model Primary School

Acceptable Internet Use Statement For Staff (Teaching and Non-Teaching)

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the pupils, the staff and the school.

The school reserves the right to examine or 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 for approval.

- Pupils accessing the Internet should be supervised by an adult at all times.
- All pupils are made 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.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/UICT Co-ordinator.
- In the interests of system security, staff passwords should only be shared with the network manager.
- Internet activity, during school hours, should be appropriate to staff professional activity or the pupil's education;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- 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-mail 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; Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Encrypted pens should be used for the storage of any School data, relating to pupils or teachers.

I agree to the terms of the Acceptable Use Agreement.

Signed _____ Date _____

Surface Pro/Laptop/Ipad Agreement for Enniskillen Model Primary School teachers

- The device remains the property of Enniskillen Model Primary School.
- The device is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Enniskillen Model Primary School staff should use the device.
- If a teacher leaves the school's employment, the device is returned to Enniskillen Model Primary School. Staff on extended leave of over 6 weeks should return their laptop/ipad to the school (other than by prior agreement with the Principal).
- When in school and not being used, the laptop/ipad must not be left in an unlocked, unattended classroom.
- Internet sites visited will often be stored on the device. Please let the UICT co-ordinator know immediately if you are worried about the content of any of the sites viewed.
- Whenever possible, the laptop/ipad must not be left in an unattended car. If there is need to do so, it should be locked in the boot.
- The laptop/ipad must not be taken abroad, other than part of a school trip, and its use agreed by prior arrangement with the Principal, with evidence of adequate insurance.
- Staff may load their own software onto the device, but it must be fully licensed and not corrupt any software or systems already installed on the device.
- Any software loaded must not affect the integrity of the school network.
- If any removable media is used (e.g. disks, memory pens) the device must be checked to ensure it is free from viruses.
- It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the device is kept up to date. (Recommendation – put the laptop on the school network at least once every month, except for summer holidays).
- Staff should not attempt to significantly alter the computer settings, other than to personalise their desktop working area.
- Pupils should not use the laptop/ipad, unless given permission by the teacher in class. (Please remember the device is still the responsibility of the teacher.)
- If any fault occurs with the device, it should be referred immediately to the UICT Co-ordinator or technician.
- The device should be covered by normal household insurance. If you are not happy that this is the case, please keep the device locked up in school overnight.

I understand and will abide by the use of Surface Pro/laptop/iPad regulations outlined above, in conjunction with the school's ICT Policy, E-Safety Policy and Child Protection Policy. I further understand that should I commit any violation the School may ask me to return the device and school disciplinary or legal action may ensue. I agree to periodically hand in my device for routine maintenance, security up-dating and screening.

Teacher _____ Date _____

Surface Pro Number _____

Internet Streaming Acceptable use Agreement Overview

The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked. Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What is Different?

Previously, primary schools had no school control over the internet sites available, and post-primary and special schools had access to a number of internet "amber groups" to which users could be added. The new system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:

In addition to the default sites, schools can choose to make users members of one or more internet-related security groups. These are:

- Internet Social Networking
- Internet Streaming Media
- Internet Advanced

Access to these groups is controlled by the C2k Manager who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL.

Internet Streaming

This group provides access to YouTube, BBC iPlayer, Vimeo and other television and radio streaming sites. When a user is added to the Internet Streaming security group the following categories, RED in the Default policy, are now GREEN.

Enniskillen Model Primary School Implications

If a member of staff is to be added to the Internet Streaming groups they must agree to the following:

- To check all video that is to be shown to classes before use
- Be responsible for the content of any video shown to a class
- To use in an appropriate manner and in accordance with the guidelines detailed in the school's Online Safety Policy and Child Protection Policy

I agree to the terms of the Internet Streaming Acceptable Use Agreement and wish to be added to this group.

Signed _____ Date _____

Reviewed October 2024

Enniskillen Model Primary School Key Points for Internet & Digital Technologies.

Our full E safety and Acceptable use of the Internet & Digital Technologies Policy is available from the office (last reviewed in 2021).

What is the Internet?

The Internet is a huge network of computers making a worldwide community. It is a way of connecting computers together so that people using them can:

 Talk to each other and have fun.

 Send and receive messages.

 Obtain information and resources.

 Publish information.

 Buy and sell things.

Why do we use the Internet in school?

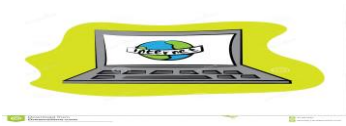
The Internet is a unique and exciting resource. It brings the world into the classroom. It has many educational benefits.

·It gives children opportunities to find up to date information that might otherwise be unavailable in school.

·It provides fast and efficient communication.

·It encourages independent learning and children enjoy using it.

The use of the Internet is an essential skill for children as they grow up in the modern world.



What are the Dangers for my Child using the Internet?

The Internet is available to all. This can bring young people into contact with unsuitable individuals.

Children should be taught that:

- People they encounter on the Internet are not always who they say they are
- They should never give personal details to a stranger on the Internet.
- They should never arrange to meet anyone contacted via the Internet on their own.

Some material on the Internet can be inappropriate for children as it may contain unsuitable information or images. Children need to know how to respond to unsuitable materials or requests on the Internet. They should be taught:

- To tell an adult immediately if they find unsuitable material.
- To tell an adult immediately if they are requested to do something that makes them feel worried and/or uncomfortable.

What can we do in School?

In our school we do everything we can to protect children using the Internet:

 All access to the Internet is provided through a filtered service.

 Internet use is supervised by an adult.

 The use of the Internet is a planned activity and websites are pre-viewed by teachers.

 Children are taught Internet safety rules.

What can you do at Home?

It is important to promote Internet Safety in the home and to take an interest in what your children are doing on the Internet.

 Keep the computer in an area of your home where you can see your child using it.

 Keep an eye on the clock! Too much time spent on the Internet can be unhealthy.

 Remind children that there are websites which are unsuitable. If they come across unsuitable materials, they must tell you.

 Know the SMART rules for Internet safety and discuss them with your children.

 Read and discuss carefully with your child/children, the rules for Responsible Use of the Internet.

Safety Rules for Children

Follow These SMART TIPS

S **Secret -** Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

M **Meeting** someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

A **Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

R **Remember** someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

T **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees