

Enniskillen Model Primary School

Acceptable use of the Internet & Digital Technologies Policy



Next review date: September 2021



Enniskillen Model Primary School

Acceptable use of the Internet and Digital Technologies

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.

Introduction

"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." DENI circular 2007/1

This document sets out our policy and practices for the safe and effective use of the Internet in Enniskillen Model Primary School. The policy has been drawn up by the staff of the school under the leadership of the Principal & UICT Co-ordinator.

In Enniskillen Model 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. Enniskillen Model PS provides pupils with opportunities to use the excellent resources on the Internet as part of their learning experience, along with developing the skills necessary to access, analyse and evaluate those resources.

This policy has been approved by the Enniskillen Model Primary School Board of Governors. Parents have been made aware of and have access to a copy of this policy.

Technology and communications are rapidly changing and becoming more sophisticated. New challenges, threats and legal requirements emerge regularly. E- Safety has become a very important issue that is essential to address in school throughout different areas of the curriculum, ensuring that all children and adults remain safe and in control when using technology.

Consequently, this policy and its implementation will be reviewed on a regular basis.

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.

Staff are allowed to take digital / video images to support educational purposes, but those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

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)

Storage of images

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.

School Website

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.)

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 discipline policy and child protection procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

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.



MOBILE PHONES

Enniskillen Model Primary School does not advocate the use of mobile phones by children in school or on trips. An exception of this is made for Key stage 2 residential trips when there is very tightly controlled access to the technology with a parental signature required.

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.

CODE OF CONDUCT FOR USE OF THE SCHOOL'S INTERNET/E-MAIL FACILITIES

This code of conduct applies at all times, in and out of school hours, whilst using school equipment. Internet access will be provided for all children to use with a responsible adult provided this code is followed. At all times the Internet should be used in an appropriate and responsible manner.



THE CODE

You SHOULD:

- Only access sites that your teacher/assistant has said you may use.
- Check with a teacher/assistant for permission before you send any messages online.
- Check with a teacher/assistant what you should do if a message appears on the screen in a pop-up box.
- Be polite about other people's work on the Internet.
- Always tell your teacher/assistant if you ever see, hear or read anything which makes you feel uncomfortable while using the Internet or e-mail.
- Ask permission from the teacher before printing.
- Only photograph or film people with their permission and only when the teacher/assistant tells you to using school equipment.
- Inform and be able to say where they have sourced information from when using the internet.

You SHOULD NOT:

- Copy text or pictures from the Internet and hand it in to your teacher/assistant as your own work.
- You should not use the words or pictures that you see on an Internet site without saying where you got it from.
- Give your name, home address, telephone numbers or any personal information about yourself or others to anyone you write to.
- Arrange to meet strangers who approach you whilst on the computer; anyone can pretend to be someone else. Someone pretending to be a friend may not have your best interests at heart.
- Give your e-mail login and password to anyone else.
- Send or look for nasty messages or pictures - tell your teacher if you see anything that upsets you.
- Download games or other programs from the Internet or bring them in from home.
- Use nasty or upsetting words when typing on the Internet.
- Intentionally cause damage on or to the computer system, or waste resources.
- Access the Internet out of class time without a teacher/assistant being present.

Please note:

You should always log out when your session has finished.

Please follow this code or your access to the Internet will be restricted.

Signed by child _____

Signed by parent _____



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;
- 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.

Signed _____ Date _____

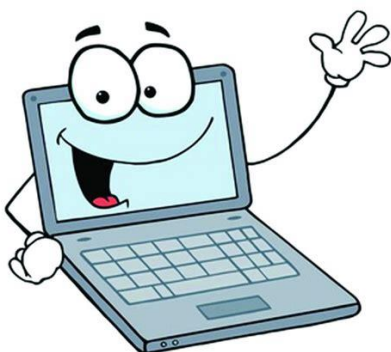
Laptop Agreement for Enniskillen Model Primary School teachers

- The laptop remains the property of Enniskillen Model Primary School.
- The laptop 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 laptop.
- If a teacher leaves the school's employment, the laptop is returned to Enniskillen Model Primary School. Staff on extended leave of over 6 weeks should return their laptop to the school (other than by prior agreement with the Principal).
- When in school and not being used, the laptop must not be left in an unlocked, unattended classroom.
- Internet sites visited will often be stored on the laptop. 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 must not be left in an unattended car. If there is need to do so, it should be locked in the boot.
- The laptop 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 laptop, but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
- Any software loaded must not affect the integrity of the school network.
- If any removable media is used (e.g. disks, memory pens) the laptop 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 laptop 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, unless given permission by the teacher in class. (Please remember the laptop is still the responsibility of the teacher.)
- If any fault occurs with the laptop, it should be referred immediately to the UICT Co-ordinator or technician.
- The laptop should be covered by normal household insurance. If you are not happy that this is the case, please keep the laptop locked up in school overnight.

Teacher _____

Date _____

Laptop Number _____



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

Our full 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 Code of Conduct.



The Smart Rules for Internet Safety are:



S

Safe - Keep safe and don't give out personal information to people you chat with online. Always keep your name, school name, home or school address, mobile or home phone number, email address and password private - it's like giving out the keys to your home!



M

Meeting - someone you have contacted on the internet 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

Reliable - sometimes people 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.