ANTRIM PRIMARY SCHOOL

-

Acceptable use of the Internet & Digital Technologies Policy

Next Review Date: Sept 2026

Antrim 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.

Introduction

The above DENI circular 2007/1 states that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

This document sets out our policy and practices for the safe and effective use of the internet in Antrim Primary School. The policy has been drawn up by the staff of the school under the leadership of the Principal.

In Antrim 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.

Antrim 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 Antrim Primary School Board of Governors. Parents have been made aware of and have access to a copy of this policy on our school website.

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.

General Information

- The use of ICT in Antrim Primary School must support the aims of the Northern Ireland Curriculum.
- Users must comply with all copyright laws.
- In school, all users must limit their use of the Internet for school related purposes. Examples of this include the use of email, the use of the Internet to investigate and research school subjects and members of staff using the Internet to further their professional development.
- All users are expected to behave in an appropriate manner when communicating with others.
- All users must be aware that the use of the Internet in schools is a privilege and not a right and this privilege may be withdrawn if it is misused.

- All users must respect the hardware and software that has been made available to them.
- All users must respect the work of others.
- All users (teaching, non-teaching and pupils) have access to the Internet through C2k network and C2k wireless.

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 Antrim 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 and other smart devices) are 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 Antrim 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, the Vice Principal). 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. Antrim 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 of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

The following key measures have also been adopted by Antrim PS 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 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.
- Pupils must not enter the folders or files of anyone else.
- Pupils must be aware that teachers have the right to enter any pupil folder. In their own class.
- The UICT Co-ordinator and Senior Leadership Team reserves the right to enter any pupil's folder.
- Pupils must not use the Internet for unapproved purposes.

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances. The school will work closely with C2K to ensure any E-Safety issues occurring through internet use are passed to the service desk team to remove and quarantine immediately.

During school hours pupils are forbidden to play computer games or access social networking sites, unless specifically assigned by the teacher.

Mobile Phones / Smart Devices

Mobile phones, alongside other smart devices (including smart watches) are changing the way and speed in which we communicate. They can provide security and reassurance; however, there are also associated risks. The inappropriate use of smart devices can disrupt lessons, interfere with teaching and learning or be used as a form of bullying-type behaviour. The potential for misuse of smart devices with recording technology is a major cause for concern.

The use of mobile phones or other smart devices by pupils is not normally permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff. Parents should encourage pupils not to bring their mobile phones into school unless it is necessary for use after school time and before the child returns home. Any mobile phone brought into school should be turned off and kept in the child's school bag. The school is not responsible for the loss, damage, or theft of any smart device. No image or sound recordings should ever be made on these devices of any member of the school community.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Positive Behaviour Policy. Minor incidents will be dealt with by the Principal or Vice Principal. 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.

Information for Parents

- Parents should be aware that the access to the internet provided to staff and pupils in school has extensive security features.
- Parents should be aware that the use of the internet in school is closely monitored by staff and that there would be no use of the internet without the supervision of staff. It would be good practice to model this at home and to place any home computers/digital devices in a public area.
- Through our use of the preventative education, students will be aware of the importance of online safety.
- Engage in positive conversations about digital literacy with your child.
- Monitor and set limitations for internet and screen time. Liaise with your Internet Service Provider (ISP) to set up age-appropriate filters/time restraints for your home Wi-Fi.
- Parents should, in cooperation with staff, make pupils aware of expectations within this document.
- Parents should be aware that the use of ICT is an integral part of teaching and learning - i.e. the use of computers/iPads in the classroom.
- Parents should be aware that children's full names will not be available online at any stage.
- Parents should be aware that no individual photographs of pupils will be available online without parents giving their permission. A data capture request is sent out to all parents at the beginning of each academic year to complete and update.
- Parents should discourage pupils from bringing mobile phones/smart devices to school on the grounds that Internet access becomes very difficult to police.

Internet Safety Awareness

In Antrim PS we believe that, alongside having a written online 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.

Internet Safety Awareness for pupils

Rules for the Acceptable use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, pupils are educated on Internet Safety Awareness using a range of online resources.

We all deserve to be able to use the internet to learn, explore and connect with each other. But all of us need to be aware of the risks involved in doing so, especially on social media. Our advice is:

- *Don't share personal information or images with people you don't know.*

- *Don't accept friend requests with someone you don't know - not everyone online may be who they say they are.*
- *Set privacy settings on all devices so that only people you know can view your account.*
- *Don't post anything online that you are not happy to be shared. It may seem like a bit of fun with friends at the time but there is always a chance those images could be shared or get into the wrong hands and could lead to harmful situations.*
- *If someone has made you feel uncomfortable or you have had disturbing interaction online, tell the police or a trusted adult. You can ring the police on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.*
- *The internet is a great place, but it is important to remember there are people out there who may wish to abuse, exploit, intimidate or bully you online - if this happens to you, tell someone immediately.*
- *Remember that if things do go wrong online, there are people who can help.*
- *If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further incidents. You will not get into trouble.*

(DENI, 2015/06)

Internet Safety Awareness for staff

The UICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and attends relevant courses that are offered. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants as appropriate.

Internet Safety Awareness for parents

The Internet Safety Policy and Code of practice for pupils is sent home for parental signature. Internet safety information for parents and carers is also sent home via the Safer School's app and Knowsley Learning Centre Online Safety newsletters.

Health and Safety

Antrim PS has attempted, in so far as is possible, to ensure a safe working environment for pupils and teachers using ICT resources in classrooms and the multipurpose rooms. Pupils are supervised at all times when the Interactive Whiteboards or Panels are being used. In the interests of health and safety, staff and students are not permitted to have food and drinks near digital devices.

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.

Parental permission is sought to cover the use of photographs of pupils on the school website, in the local press and for displays etc within school and written permission must be obtained from parent/carer.

Storage of images

Digital and video images of pupils are taken with school equipment. Images are stored on a centralised area on the school network, accessible only to school staff.

School Website and Social Media

Our school website and social media platform provides up to date information about the school, as well as giving pupils an opportunity to showcase their work. Other aspects of school life will also be highlighted on the school website or social media platform. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- 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.

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 cyberbullying 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.

As part of Online Safety education, pupils understand that social media accounts, including TikTok, Facebook, Instagram, WhatsApp, etc, are age restricted accounts. All pupils should understand that it is illegal for them to hold their own social media accounts. Antrim Primary does not support the use of age restricted social media accounts outside of school. With the exception of SeeSaw, all staff are advised not to have contact with parents and/or children on any social networking site. If a pupil attempts to communicate or befriend a staff member online it must be reported immediately to the Principal.

Staff understand and are aware that safe practice involves using judgement and integrity about behaviours in places other than the work setting, including online. Adults should not upload or add any images, video, sound or text that could upset or offend any member of the school community.

Pupil C2K email, Seesaw and Educational App Passwords

To enable pupil access to C2K devices in school all pupils are assigned a unique C2K email address and password. The email address is automatically generated through SIMS and the password is managed by the C2K manager. Seesaw and other educational apps also require pupil specific passwords and, in some cases, QR codes. Passwords for email, online learning and apps are set up at the start of the academic year and can be changed throughout the year if a breach of privacy occurs or the account becomes compromised. It is the teacher's responsibility update individual pupils of their new passwords.

Through Antrim Primary School's E-Safety and acceptable use preventative curriculum, pupils are taught to never:

- Share their password
- Attempt to gain another pupil's password
- Attempt to guess or 'hack' another pupil's account
- Access another account and make changes to the account
- Access any account, apart from their own

Any potential compromises of accounts will be investigated by the ICT coordinator and Principal. Appropriate E- Safety measures will be put in place to protect pupils.

Staff Use of Email

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of E-Safety. All emails are secured through the C2k filtering and security system. Every staff member is given SIMS generated C2K email address. Staff are expected to use their C2k emails at all times for correspondence related to school.

- Staff should not share their email addresses with parents / guardians or pupils, exceptional circumstances may apply.
- Staff are required to change their passwords when prompted by C2k and to keep these passwords confidential
- Where it is suspected that there has been inappropriate use of email by a staff member, the Principal has the authority to revoke the access of that user.
- Staff may add their C2k email to a personal mobile device or school iPad. The device should be secured with a pin code / fingerprint.

Artificial Intelligence

- **Acceptable Use**: Staff and pupils must use Generative AI tools ethically and transparently, ensuring that any AI-generated content used in schoolwork is clearly attributed to avoid plagiarism
- **Data Privacy**: No personal or sensitive data regarding pupils, staff, or school operations should be entered into AI prompts, as these tools often store data externally in ways that may not comply with the school's Information Asset Register or UK GDPR.
- **Critical Evaluation**: Pupils will be taught to critically evaluate AI-generated outputs for bias, inaccuracies, and misinformation as part of the "Using ICT" and "PDMU" curriculum.
- **Age Restrictions**: The school will enforce age-related terms of service for AI platforms to ensure pupils only access tools appropriate for their developmental stage.

Childnet International

BE SMART ONLINE



S SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

THINK U KNOW

A ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**

BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

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

Please discuss the following points with your child and sign below.

Primary 1 – Primary 2

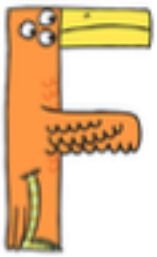
Antrim Primary E-safety agreement form



I will only use the Internet with an adult's permission and when an adult is in the room.



I will only click on icons and links when I know they are safe.



I will never tell anyone online my name, address, telephone number or passwords.



If I see something I don't like on a screen, I will always tell an adult.

My Name: _____

Parent Signature: _____



Think before you click

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.

Primary 5 – Primary 7

THE CODE

You SHOULD:

- Only access sites that your teacher has said you may use.
- Check with a teacher for permission before you send any messages online..
- Check with a teacher 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 or another adult 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 tells you to.

You SHOULD NOT:

- Copy text or pictures from the Internet and hand it in to your teacher 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 over break or lunchtimes without a teacher being present in the room.

Please note:

You should always log out when your session has finished.

Please follow this code or you may not be allowed to use the Internet again.

Signed by child: _____ Class: _____

Signed by parent: _____ Date: _____

Antrim Primary School

Acceptable Internet Use Statement For Staff

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 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/ICT teacher leader.
- 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 Antrim Primary School teachers

- The laptop remains the property of Antrim 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 Antrim Primary School staff should use the laptop.
- If a teacher leaves the school's employment, the laptop is returned to Antrim 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 ICT 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 (eg, 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 ICT Co-ordinator.
- 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: _____