CUMBER CLAUDY PRIMARY SCHOOL

e-Safety Policy

Revised by: Mrs M Smyth & Board of Governors
Date: June 2016

Date	Policy reviewed:	Policy amended:
June 2018		
June 2020		
June 2022		

1. INTERNET SAFETY POLICY

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. Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The DENI circular 2007/01 states that:

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

This document sets out the policy and practices for the safe and effective use of the Internet in Cumber Claudy Primary School. The policy has been drawn up by the staff of the school under the leadership of Mrs Maureen Smyth/Mrs Dawn Hume Principal/ICT Co-ordinator. It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested.

The policy and its implementation will be reviewed annually.

2. C2K

Classroom 2000 (C2k) is the project responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

Some of these safety services include:

- Providing all users with a unique user names and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses Filters access to web sites
- Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

3. 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. We have a Code of Safe Practice (Appendix 1) for pupils and staff containing eSafety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, 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.**

Mrs Dawn Hume, the ICT Co-ordinator and the Principal/Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

Parent consent is obtained/updated annually (via the data capture form).

In addition, the following key measures have been adopted by Cumber Claudy Primary School to ensure our pupils do not access any inappropriate material:

- The school's eSafety code of practice for Use of the Internet and other digital technologies is made explicit to all pupils and eSafety guidelines are displayed prominently throughout the school;
- 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 Key Stage 2 are educated in the safe and effective use of the Internet, through a number of selected websites.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

The use of personal mobile devices by pupils is not permitted on the school premises.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Behaviour Policy. Minor incidents will be dealt with by the class teacher and/or the Principal and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's child protection policy.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff:

- Pupils accessing the Internet should be supervised by an adult at all times.
- Staff will make pupils 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 been granted 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 Co-ordinator.
- In the interests of system security staff passwords should only be shared with the network manager.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should, where possible, be taken with a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work.
- School systems may not be used for unauthorised commercial transactions.

4. Internet Safety Awareness

In Cumber Claudy Primary School we believe that, alongside having a written eSafety 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, P4 to P7 pupils are made aware and discuss Internet Safety through structured lessons. There are various pupil resources available such as:

Digiduck
Gridclub
Signposts to Safety (primary and secondary versions)

Key Stage 2- 4
KidSMART
Know IT All for Schools
ThinkUKnow
Childnet's Sorted website

Internet Safety Awareness for staff

Key members of staff keep informed and updated on issues relating to Internet Safety. All teaching staff and classroom assistants are in turn made aware of the Departments policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.

The Child Exploitation and Online Protection Centre **(CEOP)** runs regular one-day courses for teachers in Northern Ireland. These are advertised directly to schools. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the Thinkuknow website.

Internet Safety Awareness for parents

The Code of safe Practice for pupils (linked to this e-safety policy) is sent home at the start of each school year for parental signature. Additional advice for parents with internet access at home also accompanies this letter or Internet safety leaflets for parents and carers are sent home when available.

5. Health and Safety

In Cumber Claudy Primary School we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors.

Use of Mobile Devices

Many modern mobile devices have internet connectivity. Please refer to the schools policy on the use of mobile phones

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use Wi-Fi (Wireless Fidelity) equipment. Further information on Wi-Fi equipment is available at: the Health Protection Agency website.

6. School Web Site

The school web site is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well-presented and that personal security is not compromised. An editorial team ensure common values and quality control. As the school's Web site can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply.

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- Pupils' christian names will only be used on the website.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

The Use of Social Media- Teaching Staff

From e-mail to text and from blogging to tweets, technology is becoming an ever-present in our lives and an increasingly essential tool in the classroom. These new technologies open up a whole range of possibilities to help pupils, and others involved in their education; they provide new access to assignments and resources, connect classrooms in other communities and countries in ways unthinkable only a few years ago.

The ability to communicate in real time with others and access networks across the world brings with it great opportunities for teachers. It also offers great challenges as the boundary between teacher and pupil can quickly become blurred.

The open nature of the Internet means that social networking sites can leave professionals such as teachers vulnerable if they fail to observe a few simple precautions. The guidelines below are intended not as a set of instructions, but general advice on how to avoid compromising your professional position.

Reference to online communications and social media include software, applications (including those running on mobile devices), e-mail and websites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, LinkedIn, YouTube, Wikipedia and MySpace.

Also included is the use of SMS and instant messaging clients, such as, MSN, Messenger and BBM.

Privacy

To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly. Do not accept friend requests from a person you believe to be either a parent or a pupil at your school.

Privacy Settings- recommended security level

Send you messages- Friends only

See your friend list- Friends only

See your education and work- Friends only

See your current city and hometown-Friends only

See your likes, activities and other connections- Friends only

Your status, photos, and posts- Friends only

Bio and favourite quotations- Friends only

Family and relationships- Friends only

Photos and videos you're tagged in- Friends only

Religious and political views- Friends only

Birthday- Friends only

Permission to comment on your posts- Friends only

Places you check in to- Friends only

Contact information- Friends only

Conduct on social networking sites

As a teacher you should:

- always maintain a formal and courteous and professional tone in communicating with pupils and parents and ensure that professional boundaries are maintained; (if contacted)

- only use official work e-mail addresses when communicating with pupils or parents;

- not exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with pupils;

- firmly decline student-initiated ‘friend’ requests from pupils and do not instigate any yourself. Decline friend requests from parents and remind them of more formal channels which they can use to discuss their child’s education;

- operate online in a way in which would not call into question your position as a professional;

- realise that pupils will be naturally curious about your personal life outside school and may try to find out more about you.

- Manage your privacy setting and keep them under review. These are particularly important in regard to photos, and remember that no privacy mechanism is 100% guaranteed;

- ensure your settings prohibit others from tagging you in any photos or updates without your permission and you can ask others to remove any undesirable content related to you;

- consider that conversations held online may not be private. Be aware of who may have access to what you post;

- assume that information you post can be accessed and altered;

- not discuss pupils, colleagues, parents or carers online or criticise your employer or others within the school community;

- respect pupil privacy and confidentiality at all times;

- use strong passwords and change them regularly. Protect your mobile phone/smart phone/tablet computer with a PIN, especially when in school to protect access to its content and potential misuse;

- bring the matter to the attention of the principal using the proper procedures, if you are the victim of cyber bullying or uncomfortable with comments, photos or posts made by pupils of or about you.

The school's rules for safe Internet are outlined below.
Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Maureen Smyth, Principal.

Appendix 1

ICT Code of Safe Practice
(Primary Pupils)

eSafety Rules

I will only use ICT in school for school purposes.

I will only use my class e-mail address or my own school e-mail address when e-mailing.

I will only open e-mail attachments from people I know, or who my teacher has approved.

I will not tell other people my ICT passwords.

I will only open/delete my own files.

I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

✂ -

Parent/ carer signature

We have discussed this and ……………………………….........(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Cumber Claudy Primary School.

Parent/ Carer Signature …….................................... Date ………………………

ICT Code of Safe Practice for Staff
eSafety Rules

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. <u>This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.</u> All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Dawn Hume, eSafety coordinator or Mrs Maureen Smyth (Principal)

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, C2k, secure e-mail system for any school business.
- I will ensure that pupil data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware of software without permission of the Principal.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will adhere to the 'Social Networking Code of Conduct' for staff and volunteers at Cumber Claudy Primary School.
- I understand that I must never befriend a pupil at Cumber Claudy Primary School onto a social networking site.

User Signature
I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school

Signature ………………………………………. Date ……………………

Full Name ………………………………….... (printed) Job Title . . . .

Appendix 2

Sample Posters

Foundation Stage and Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

B. Stoneham & J. Barrett

Key Stage 2

Think then Click

- We ask permission before using the Internet.
- We only use websites that are C2k approved.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately minimise any webpage we are not sure about and tell an adult.
- We only e-mail/message people an adult has approved.
- We send e-mails or messages that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms that are not approved by C2k.

Principles for Internet Use ----- Children’s Version

Be **SMART** On Line

S	**Secret** Never give your address, telephone number, username or password when on-line.
M	**Meeting** someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher.
A	**Acceptin**g e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.
R	**Remembe**r no offensive language, text or pictures are to be displayed, sent, copied or received.
T	**Tell** your parent, teacher or trusted adult if someone or something makes you uncomfortable.

Smile and Stay Safe Poster

e-Safety guidelines to be displayed throughout the school

nd stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Additional Advice for Parents with Internet Access at home

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.

2. Parents should agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use;

4. Parents should get to know the sites their children visit and talk to them about what they are learning;

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below);

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.
- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)
- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use.