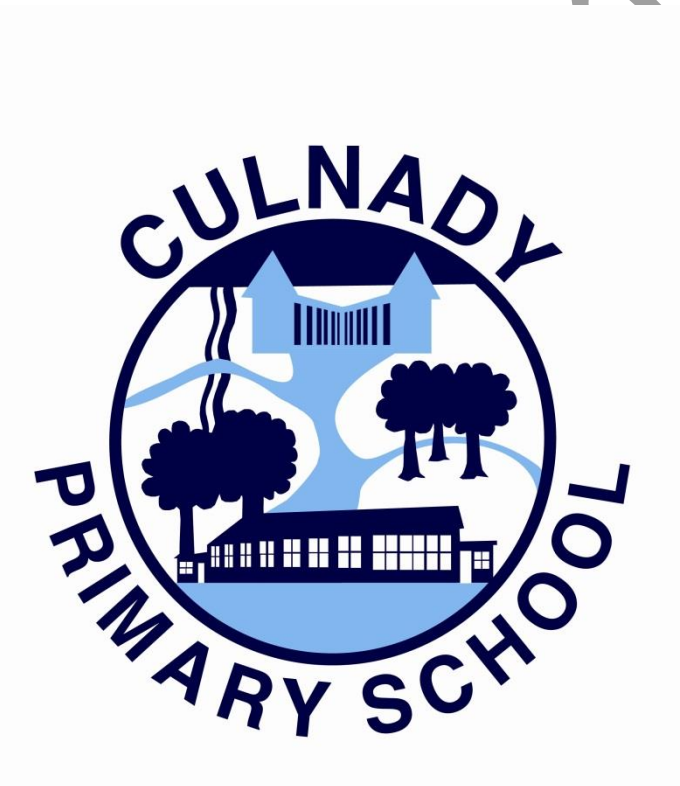
CULNADY PRIMARY SCHOOL



Acceptable Use of ICT Policy

Policy for the safe, healthy, acceptable and effective use of the Internet and other digital technology tools

1.0 Management Responsibility

This policy outlines our purpose in providing safe, healthy, acceptable and effective access to the Internet and in using other digital technology tools in Culnady Primary School. Whilst there are enormous benefits for children using the internet and other digital technology tools, at home and in school, there are potential dangers for children using them unsupervised. This policy explains how our school is seeking to avoid the potential problems that unrestricted use could give rise to and how these very powerful resources can enhance and potentially transform teaching and learning when used effectively and appropriately.

The technologies that this policy refer to include: fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, ipads, webcams and digital video equipment); as well as technologies owned by pupils and staff, but brought onto school premises (such as mobile phones, camera phones, personal digital assistants (PDAs), and portable media players). Children are not permitted to bring personal digital equipment into the school unless in exceptional circumstances and agreement to do so has been permitted by the school Principal. The use of devices owned personally by staff and pupils is subject to the same requirements as technology provided by the school.

2.0 Internet access and other digital technology in school

Teachers and pupils will have access to world-wide websites offering educational resources, news and current events. There will be opportunities for discussion with experts and to communicate and exchange information with students and others on a global scale.

In addition, staff will have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the EA and DENI; receive up-to-date information and participate in government initiatives.

In the longer term the Internet may also be used to enhance the school's management information and business administration systems.

3.0 Ensuring Internet access is appropriate, safe and effective

The Internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet.

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet access is provided by C2k and provides a service designed for pupils including a "firewall" filtering system intended to prevent access to material inappropriate for children;
- Children using the internet will normally be working in the classroom, during lesson time and will be supervised by an adult (usually the class teacher) at all times;
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;
- KS2 pupils will be taught to use e-mail within the school network. Children will have permission from parents to use e-mail on the school system.
- Our Rules for Responsible Internet Use and e-mail will be posted near computer systems.
- The ICT co-ordinator will monitor the effectiveness of internet access strategies;
- The ICT co-ordinator will ensure that occasional checks are made on files to monitor compliance with the school's Acceptable Use of ICT Policy;
- The Principal will ensure that the policy is implemented effectively;

- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the EA, CCEA, C2k and DENI.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen.

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the ICT Co-ordinator and the Child Protection Officer in consultation with the Principal and the pupil's class teacher. All the teaching staff will be made aware of the incident at a Staff Meeting if appropriate.

- If one or more pupils discover or view inappropriate material our first priority will be to give them appropriate support. The pupil's parents/guardian will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/guardians and pupils to resolve any issue;
- If staff or pupils discover unsuitable sites the ICT co-ordinator will be informed. The ICT co-ordinator will report the URL (address) and content to C2k and the EA who will take the appropriate measures according to their policies.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use (Appendix 1) and following the SMART Tips (Appendix 2) which have been designed to help protect them from exposure to internet sites carrying offensive material. If pupils abuse the privileges of access to the internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to the Internet may be denied for a period.

3.2 Internet Safety Awareness for School Staff

During work, staff and any supply staff, are also expected to play their part in using the internet responsibly by following the Rules for Responsible Internet and Technology Use for Staff (Appendix 3).

Staff will not be expected to take charge of an Internet activity without Internet Safety Awareness training. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the internet, will be provided with this policy (Acceptable Use of ICT); the document 'Safeguarding children in a digital world' provided by BECTA and will have its importance explained to them.

3.3 Using the Internet to enhance learning

Pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will begin to use the Internet to find and evaluate information. Access to the Internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher or classroom assistant demonstration;
- Pupils may access teacher-prepared materials, rather than the open internet;
- Pupils may be given a suitable web page or a single web site to access;
- Pupils may be provided with lists of relevant and suitable web sites which they may access.

- Older more experienced pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher;
- pupils will be expected to observe the Rules of Responsible Internet Use and will be informed that checks can and will be made on files held on the system and the sites they access.

Pupils accessing the Internet will be supervised by an adult, normally their teacher at all times. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

3.4 Using information from the Internet

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it is copyright.

- pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium);
- when copying materials from the Web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

KS2 pupils will learn how to use an e-mail application and be taught e-mail conventions. Staff and pupils will begin to use e-mail to communicate with others, to request information and to share information.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- Pupils will only send and receive emails through C2K child friendly online e-mail accounts;
- Pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use;
- Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Incoming e-mail to pupils will not be regarded as private;
- Children will have the content of the e-mail messages they send checked by the teacher.
- All emails sent by pupils can be accessed by the Principal and ICT co-ordinator when required.
- Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

4.0 School website

Our school website is intended to:

- Provide accurate, up-to-date information about our school;
- Promote our school
- Celebrate good work;
- Provide pupils with the opportunity to publish their work on the internet.

All classes may provide work for publication on the school website. The ICT co-ordinator is responsible for up-loading pages to the school website, ensuring that the links work and are up-to-date, and that the site meets the requirements of the site host.

The point of contact on the website will be the school address, telephone number and e-mail address.

The following safe guards will be employed with regards to our school website:

- Class teachers will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained.
- All material must be the author's own work.
- Parental permission will be sought for use of pupils' photographs throughout the school year before using images of pupils on the website or elsewhere.
- Home information or individual e-mail identities will not be published.
- Staff will be identified by their title and surname unless they request otherwise.

School Website address www.culnadyps.co.uk

5.0 Internet access and home/school links

We will keep parents in touch with future ICT developments by newsletter.

Internet use in pupils' homes is rapidly increasing and some parents may be grateful for any advice/guidance that the school can offer – especially with regard to safe access for children. The ICT co-ordinator is willing to offer advice and suggest alternative sources of advice on the understanding that neither he/she, nor the school can be held responsible for the consequences of such advice. Furthermore:

- A selection of leaflets and booklets offering relevant e safety guidance from organisations such as BECTa, PSNI, CEOP will be available in the school reception area.
- The school will also organise Internet Safety Workshops for parents/members of the community in partnership with the PSNI, the details of which will be made available on the school website and newsletter.

6.0 Making and storing digital and video images

Digital and video images are captured and stored within the school, and the guidelines for the protection of both pupils and staff are as follows:

If staff members use personal digital cameras or camera phones on school trips, such images should be appropriately transferred back to the school network and then deleted. The school has created a centralised area on the school's network for storing digital images of pupils, with suitable security for accessing the images, along with a deletion policy for when images are no longer required, or the pupil has left the school.

7.1 Bullying and Harassment

Bullying and harassment (cyber-bullying) can occur through mobile phones as well as online. It can often be done anonymously. Staff can also be subjected to 'cyber-bullying' by pupils. Unacceptable and threatening photographs and videos can be used. Ownership of a mobile phone may also be a cause for bullying resulting in theft.

School staff, parents and young people need to work together to prevent such behaviour and to tackle it whenever it occurs.

Pupils and Staff will be made aware of:

- How to react when threatened whether the digital medium is a mobile phone, website or email.
- Email – report to the email service provider, block the sender and change the email address.
- Websites - pages should be copied and printed from the website concerned for evidence, and the Internet service provider (ISP) responsible for hosting the site should be contacted immediately.

7.2 Social Media

- The school C2k system will block access to social networking sites (e.g. Facebook).
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of cyber bullying to the school.
- School staff will not add children as 'friends' if they use social networking sites.
- Parents will be advised not to post photos/videos on social networking sites.

7.3 Mobile phones

Use of mobile phones by children, on the school premises, is forbidden unless under special circumstances that has been sanctioned by the Principal.

Use of mobile phones by staff is restricted to appropriate designated times such as staff break and lunch times. These are outlined in the staff code of conduct.

8.0 Management of Information Systems

8.1 Managing and reporting incidents and securing evidence of misuse
To deal with any incidents of technology misuse which arise, procedures have been devised, which are based on the existing school behaviour policy, rules, regulations and established practices. These incidents may involve pupils, teaching or non-teaching members of staff.

Minor incidents will be dealt with by the ICT coordinator. Others more serious or illegal incidents will be dealt with by the Principal and Governors.

Incidents which might be described as minor, involve plagiarism or copyright infringement, downloading materials or images not relevant to the subject, using someone else's password or sending nuisance text messages.

More serious examples might involve soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes and cartoons or material which is libellous or intended to harass.
Where the incident involves child abuse, the Designated Teacher for Child Protection in the school will also be notified and the school will follow the reporting procedures as set out in the Child Protection Policy.

Harassment of another person using technology, or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences.

If the school identifies a suspect computer (containing for instance indecent images or offences concerning child protection), it should not be used or viewed and advice on how to proceed will be sought from the local PSNI hi-tech crime unit.

If police involvement is necessary, the Principal and Board of Governors will seek legal advice, via their normal sources, as soon as possible.

After a minor or major incident a comprehensive debriefing will occur to review school policy and procedures, to make and monitor any necessary changes and to maximise what can be learnt.

8.2 Use of school systems for commercial purposes
School systems may not be used for unauthorised commercial transactions.

Neither teachers nor pupils should use the IT facilities for private financial gain or for commercial purposes. Systems must not be used to offer, provide or purchase products or services unless prior approval to do so has been given by the Principal.

9.0 Health and Safety

9.1 Safe location and supervision of computers in schools

Internet access for pupils is available on computers that are in highly-used areas of the school.
Computer screens are visible to other people circulating in the area and while using the Internet at school, pupils are, where possible, supervised.
However, when appropriate, pupils may be given permission to use systems independent of staff supervision. In all cases, pupils should be reminded, through visible notices, of their responsibility to behave in line with the school code of practice.

9.2 Physical health matters to consider when using technology devices

The three problems that can be caused by using a computer are:

1. Musculoskeletal – this is usually aches and pains in the neck, shoulders, arms or back.
2. Visual fatigue – tired or sore eyes and headaches.
3. Stress – caused by problematic software.

Staff have been provided with a document called 'safe computer use' which highlights techniques to minimise the impact of computer use on their health.

9.21 Interactive Whiteboards and Projectors

All interactive whiteboards and other data projectors, if misused, have the potential to cause eye injury, particularly if children stand in front of the beam to give presentations. The following guidelines should be followed:

- Make clear to all users that no one should stare directly into the beam of the projector.
- When entering the beam, users should not look towards the audience for more than a few seconds.
- Encourage users to keep their backs to the projector beam when standing in it.
- Children should be supervised at all times when a projector is being used.

9.22 Photosensitive epilepsy

Using a computer is unlikely to be a problem for people with photosensitive epilepsy as the screen flicker is higher than the rate that triggers epilepsy. However, to make sure that any possible risk is kept to an absolute minimum, it is important to consider both the type of software and the display screen.

10.0 e-Learning

10.1 What is e-Learning?

This is learning that is made possible and supported through the use of Information and Communications Technology (ICT) in school and at home. Whatever the technology being used by the individual learning, it is at the core of the educational journey. Undoubtedly, e-Learning involves engaging in a wide range of learning activities, both inside and outside school, including the use of ICT to support life-long-learning for families. Schools involved in e-Learning use a mixture of familiar learning techniques and traditional methodologies combined with e-Learning that is delivered entirely online.

10.2 What is a VLE?

We will be developing a Virtual Learning Environment (VLE) in Culnady Primary School. A VLE is a Web-based platform for the digital aspects of courses of study. We will be using a variety of child friendly platforms including C2K's Fronter and Learning NI. The advantage of online learning means that it can be accessed from anywhere in the word and at any time.

10.3 What is in a VLE?
Generally VLEs contain the following features:

- communication tools (email, bulletin boards and chat rooms);
- collaboration tools (online forums, intranets, electronic diaries and calendars);
- tools to create online content and courses;
- online assessment and marking;
- controlled access to curriculum resources; e.g., Newsdesk, online educational videos and an area to store files

10.4 e-Learning in our school
The school has a managed computer service supported by C2K which provides us with computers, laptops and ipads. We have Interactive Whiteboards in every classroom. We have a network that allows children to access their individual documents, the internet and a local printer to support their eLearning skills development.

10.5 e-Learning at home
If you have an internet connection at home, we encourage your child to access LNI using their C2K username and password. This enables them to interact with age appropriate learning resources in a safe and controlled way.

APPENDIX 1

ICT Code of Practice Agreement for Pupils and Parents

All the computers in the school network have access to the internet to help our learning. These rules will help keep us safe and help us be fair to others.

Using the Computers:

- I will only access the computer system with the login and password I have been given;
- I will not access other people's files;
- I will not bring in memory sticks or CDs from outside school and try to use them on the school computers, unless I have permission from the teacher.

Using the Internet:

- I will ask permission from a teacher before using the internet;
- I will only use the websites given to me by the teacher unless I am given permission to use a search engine.
- I will report any unpleasant material to my teacher **immediately** because this will help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the internet sites I visit;
- I will never give or send anyone my full name, my home address or telephone number when using the internet.

Using e-mail: (KS2)

- I will ask permission from a teacher before using e-mail in school;
- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I receive or send may be read by a teacher;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.
- I will respect the rules for using e-mail and understand that the e-mails I send to others are stored on the school network.

*Now read the SMART tips to stay safe online.

We have read the ICT Code of Practice and SMART Tips and agree to follow them

Signed by child _____

Signed by parent/guardian _____

Date _____

Culnady Primary School

Safety Tips for Responsible Internet Use for Pupils

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

Culnady Primary School
Rules for Responsible Internet and Technology Use for Staff

The computer system is owned by the school, and may be used by staff to enhance their professional activities including teaching, research, administration, on-line learning and management. The school's ICT Acceptable Use 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 using Internet access and other digital technologies must accept and comply with the following guidelines.

Use of the Internet:

- All Internet activity should be appropriate to staff professional activity or the students' education;
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Use of the network for accessing, creating, retrieving, downloading, sending, copying, printing or displaying inappropriate materials such as pornographic, racist or offensive material is forbidden.

Use of e-mail:

- Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received;
- 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.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Use of obscene or racist language should not be used.
- Technology should not be used to harass, insult or attack others.

Use of computer Network:

- Staff should avoid damaging computers, computer systems or computer networks.
- Trespassing in another user's folders, work or files is forbidden.
- Staff should not intentionally waste ICT resources.
- The use of personal social media (e.g. Facebook, Twitter etc.) is not permitted in school.
- Staff should be aware that C2k record sites visited, searches made on the Internet, emails and messages sent and received by individual users.
- The school code of conduct relates to use of school laptops or the use of school equipment at home e.g. ipads

Use of Digital Cameras:

- Digital images or video images must be stored in the allocated area on the school network.
- Digital images taken on personal devices must be transferred to the allocated area on the school network and then deleted.
- Digital images taken in school should not be stored on personal computers.
- Parental permission to photograph pupils is required.

Use of Mobile Phones:

- During the working day making phone calls or sending text messages must only be carried out during staff break and lunch times.

We have read the Rules for Responsible Internet and Technology Use for Staff and agree to follow it

Name of Staff Member _____

Signature _____

Date _____