Drumhillery Primary School

E-Safety Policy
&
Acceptable Use Agreement

Policy Review
Date: September 2018
Next Review: September 2019
Signed By: _____ Chair of Board of Governors
_____ Principal _____ ICT Co-ordinator
_____ Designated Child Protection Teacher

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circulars 2011/22, 2013/25 and 2016/27 on e-Safety. This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Drumhillery Primary School. It also links to Article 17 from the UN Convention on the Rights of the Child which states:

"You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure the information you are getting is not harmful, and help you find and understand the information you need."

Introduction

UICT (Using Information and Communications Technology) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality such as iPads and tablets

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

At Drumhillery Primary School we endeavor to provide pupils with the opportunity to access the internet and use web-based learning opportunities. This policy outlines our purpose in providing e-mail facilities

and access to the internet at our school and explains how we seek to avoid the potential problems that unrestricted internet access could give rise to.

We understand the responsibility to educate our pupils in E-Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. All users must comply with all relevant legislation on copyright, property, theft, libel, fraud, discrimination and obscenity.

What is E-Safety

E-Safety is short for Electronic Safety. It encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. E-Safety highlights the need of the school, staff and parents to educate children and young people about the benefits, risks and responsibilities of using information technology.

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. The main risks for the school setting can be categorized as Content, Contact and Conduct of Activity.

Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia. Some information is illegal, harmful and there is an inability to evaluate the quality, accuracy and relevance of it.

We aim to teach children:

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Contact

Children may meet someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons. There is a risk of being subject to grooming by these individuals. Cyber-bullying, unauthorized access to/loss of/sharing of personal information can all take place.

We aim to teach children:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details.
- That they should never meet alone anyone contacted via the Internet.
- That once they publish information it can be disseminated with ease and cannot be destroyed.
- That they should never post or share personal information or photographs at the request of a stranger.

Conduct

Online activity has the potential for excessive use which can impact on the social and emotional development and learning of children. Plagiarism

and copyright infringements along with illegal downloading of music and video. The sharing and distribution of personal images without an individual's consent or knowledge can all lead to criminal offensives and records.

We aim to teach children:

- The importance of our own personal data and information.
- Respect for all.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

We aim to teach children:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

Cyber Bullying

Children may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying, if it takes place within school, will be considered with the schools overall anti-bullying policy, discipline policy and pastoral services provided. At present we do not use social media to aid teaching and learning and this shall continue until a time when we feel it would be beneficial to our pupils and approval is given by the principal.

Cyber Bullying can take many different forms and appearances including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones (see school Mobile Phone Policy for further information) – examples can include abusive texts, video or photo

messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.

- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal/ICT Co-ordinator update Senior Management and Governors about e-safety and all governors understand the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.

- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child. This consent remains valid for the entire period that the child attends school unless circumstances or agreements need to be changed.
- Parents/carers are required to decide as to whether they consent to images of their child being taken / used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate relevant e-Safety information through newsletters and the school website.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.

- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.
- Use parental controls on all devices and check privacy settings continually as these do change regularly with updates.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective; therefore, all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Staff have access to 'YouTube' (for educational purposes only) when logged into the C2K system. Staff must always ensure that no pupil is given access to a computer that they are logged on to unless supervised.
- Staff should always ensure Internet searches involving sites that have been granted enhanced access to should not be carried out when children can view them, i.e. on computer's screen or on an interactive whiteboard. 'YouTube' should only be used after the content has been viewed and checked, ensuring that children are not exposed to inappropriate content.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. They are taught to "Click Clever, Click Safe":

Zip it (Never give personal data over the Internet)

Block it (Block people you don't know)

Flag it (If you see something you don't like, flag it up with someone you trust)

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

- The school C2k system will block access to social networking sites.
- 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 bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

The school is not responsible for pupils' Facebook accounts or other social networking sites and therefore parents are advised to monitor them closely and ensure that all children's accounts are private.

It is important to note that it is against the law for children under the age of 13 to have a Facebook account.

For further information please see our Social Media Policy.

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.

- Pupils are not allowed to use personal mobile devices/phones (in school) during class.
- Staff should not use personal mobile phones during designated teaching sessions.
- Pupils are only permitted to bring electronic devices to school on special occasions. These are brought to school at the owner's own risk. These cannot be used to take photographs, videos or gain access to the internet.

Please see our Mobile Phone Policy for further information.

Managing Video-conferencing:

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

Multimedia Technology

At Drumhillery we are aware of the educational benefits the good and proper use of communication technology provides for our pupils, and we do advocate this to promote and enhance the learning of our pupils. We have 16 iPads available for pupil use. We however, are also very aware of the potential for personal harm, hurt and damage to individuals by the misuse and abuse of this technology. Consequently, the school is therefore concerned with making the provision of multimedia technology safe for both pupils and staff.

Pupil's use of iPads:

Pupils use iPads as an educational tool and this is seen as beneficial by teachers as it helps enhance learning experiences.

Pupils are not permitted to use iPads for the following:

- To send inappropriate pictures
- Send hurtful messages
- Access social networking sites (Facebook, Twitter etc)
- Access Internet without permission
- Take photos of pupils/staff without permission
- Take videos of pupils/staff without permission

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. At present we do not post images of pupils on the school's Facebook page.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the School Website or Facebook page, particularly in association with photographs. First name terms only.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.
- Staff will not use their own personal devices to take photographs or videos.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network and MIS systems.

Handling e-Safety Complaints:

To deal with any incidents of technology misuse by pupils which arise, the school's Positive Behaviour Policy will be followed. Pupils will be made aware the repeated misuse of the Internet may lead to their access to it being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.

Where the incident involves child abuse, the Designated Teacher for Child Protection/Safeguarding Children in the school will be notified and the school will follow procedures as set out in the school's Child Protection/Safeguarding Children Policy.

Issues of Internet misuse and access to any inappropriate material by any user should be reported immediately to the school's e-Safety Co-ordinator and recorded in the school's e-Safety log, giving details of the site and the time.

A record of very serious e-Safety incidents will be kept in the locked Child Protection/Safeguarding Children cabinet within school.

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.

For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed, and advice will be sought from the P.S.N.I.

After a minor or major incident, a comprehensive debriefing will occur to review school policy and procedures.

Logs of misuse, changes to filtering controls and of filtering incidents are made available to the Principal and Governors. If police involvement is necessary, the Principal/e-Safety Co-ordinator/Board of Governors will seek advice from Schools' Branch and the legal department of the Education Authority.

Communicating the Policy

Introducing the e-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.
- E-Safety Day will be held each February and e-safety will be highlighted throughout class activities and special assemblies.
- Pupils will be informed that network and Internet use will be monitored. Senior members of staff can access and view pupils' files if they deem something to be inappropriate.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct are essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use regarding Internet access, data protection and use of software, both in and out of school.
- All staff are asked to sign an Acceptable Use form and provide or withdraw permission for images of themselves to be used on the School Website and Facebook page.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

Links to other Policies:

Pastoral Care Policy

Child Protection Policy

Social Media Policy

Mobile Phone Policy

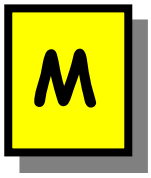
Positive Behaviour Policy

Anti-Bullying Policy

Safety Rules for Children

Follow These SMART TIPS

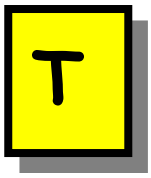
Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



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 Area Child Protection Committees

Drumhillery Primary School

Acceptable Use of the Internet

The school has installed computers, laptops, iPads and internet access to help our learning. Children should know that they are responsible for making Acceptable Use of the Internet. They must discuss and agree these rules for Acceptable Use.

Pupil Promise

- I will access the system with my login name and password, which I will keep secret and secure.
- I will not access other people's files without permission
- I will only use the computers for school work and homework
- I will not bring in, download or install software to school computers or iPads.
- I will ask permission from a member of staff before using the internet.
- I will only e- mail people I know, or my teacher has approved.
- When sending e-mails, I will not give my name, address or phone number or arrange to meet anyone.
- I will not open e- mails sent by someone I don't know.
- The messages I send will be polite and responsible.
- I will not ever use offensive or inappropriate language in message.
- I will report any unpleasant material or messages sent to me
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not attempt to access any inappropriate material.
- I will not access internet chat- rooms in school.
- I will never give out personal information or passwords to other internet users.
- I will not bring my mobile phone to school or school trips without permission.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks from home to use in school unless I have been given permission by my class teacher.
- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet/E-mail and my parents/cares will be informed.

Pupil Name: _____ Signed by Pupil: _____

Date: _____

Parent/Guardian – Consent for Use of Internet/digital images of pupils

As the parent or legal guardian of the pupil named, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions.

I am aware of the school's E-Safety policy and have circled below how I wish images of my child to be used.

I understand that my child will not be included in photographs of school activities unless this consent form is signed and returned.

Images/Video of _____ (pupil's name) may be used by the school in the following ways		
On the school's website (even after they no longer attend this school)	Yes	No
In School Publications	Yes	No
In displays in classrooms and communal areas	Yes	No
Video recordings including Special Performances	Yes	No

I recognize that it is not possible to restrict access to all controversial materials available on the Internet and I will not hold Drumhillery Primary School responsible for any improper or illegal use of the internet by my child.

I hereby give permission to permit internet access for my child and agree to the safety restrictions listed.

Print Name: _____ (Parent/Guardian)

Signed: _____ Date: _____

Drumhillery Primary School

Staff Acceptable Use Agreement

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's e-Safety Policy has been drawn up to protect all parties – the students, the staff and the school.

STAFF MEMBER: _____

- In line with Drumhillery Primary School's e-safety policy I understand: I must not engage in any on-line activity that may compromise my professional responsibilities or bring the name of the school into disrepute;
- The school has the right to monitor my use of the school's ICT systems, email and other digital communications;
- I will not search for, access, upload, download any materials which are inappropriate/illegal such as child sexual abuse images pornography, racist, sectarian or offensive material is forbidden;
- I must immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Principal or the school's e-Safety Co-ordinator;
- The use of school ICT systems for personal financial gain, gambling, political purposes or advertising is forbidden;
- I must not disclose my C2K username or password to anyone else, nor will I try to use anyone else's C2K username and password;
- I will not use the school systems to access social media sites and I will not make friend requests to pupils or accept friend requests from pupils;
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of photographs/digital images;
- I must not access, copy, remove or otherwise alter any other user's files, without their express permission; any activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- When communicating electronically with others I should be professional, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- Posting anonymous messages and forwarding chain letters is forbidden;
- The need to be cautious when opening attachments to emails, due to the risk of the attachment containing viruses or other harmful programmes;
- Copyright of materials must be respected;
- That this Acceptable Use of the Internet Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use

of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school;

- The school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the context of the school's e-Safety policy;
- I will only use my personal mobile ICT devices as agreed in the school's 'e-Safety Policy' and the school's 'Use of Mobile Phones and Related Technologies Policy';
- I should immediately report any damage or faults involving equipment or software, however this may have happened;
- That if I have been granted enhanced Internet access (details kept in the school's e-Safety log) to certain websites using the C2K system or I am using the non C2K router or 3G technology (or equivalent) I must always ensure that no pupil has access to a computer on which I am logged on (unless under my supervision).
- When using the C2K there is a log of my Internet searching history, the school reserves the right to examine or delete any files and documents that may be held on its computer system.

I understand that if I fail to comply with this Acceptable Internet Use Policy Agreement. I could be subject to disciplinary action, referred to the P.S.N.I. for further investigation and/or the procedures followed in line with the school's Child Protection/Safeguarding Children Policy.

Images/Video may be used by the school in the following ways		
On the school's website	Yes	No
In School Publications	Yes	No
In displays in classrooms and communal areas	Yes	No
Video recordings including Special Performances	Yes	No

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Signed: _____ Date: _____