E-Safety Policy

May 2015

Date ratified: 20th August 2015

E-SAFETY POLICY

1. INTRODUCTION

Boards of Governors have a duty to safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries (Northern Ireland) Order 2003). It is also the duty of the Board of Governors to determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003 refers).
In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.

This E-safety policy contains policies in relation to use of the internet. It is largely based on DENI Circulars of 2007/1 *"Acceptable Use of the Internet and Digital Technologies in Schools," 2013/25 "eSafety Guidance" and* should also be read in conjunction with the Schools Child Protection Policy.

2. 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 Donemana Primary School. The policy has been drawn up by the staff of the school under the leadership of Mrs G Hay, Principal and Mr D Potts, 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.

3. C2K

My-School (C2k) is the project responsible for the provision of 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.

4. 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.

Mr D Potts, 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

A parental/carer consent letter (Appendix 2) accompanied by the code of practice for pupils is sent out annually to parents/carers and this consent must be obtained before the pupil accesses the internet.

In addition, the following key measures have been adopted by Donemana P.S. 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 mobile phones by pupils is not permitted on the school premises during school hours. (Refer to Acceptable use policy for mobile phones and other electronic devices in Use of Images Policy 2014) During school hours pupils are forbidden to play inappropriate computer games or access social networking sites.

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 class teacher 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 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 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.

5. Internet Safety Awareness

In Donemana 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, Key Stage 2 pupils are made aware and discuss Internet Safety through structured lessons. There are various pupil resources available such as:

Signposts to Safety (primary and secondary versions)

Key Stage 2
KidSmart
Know IT All for Schools
ThinkUKnow
Childnet's Sorted website

Internet Safety Awareness for staff

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory 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) run 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 Internet Safety Policy and Code of safe Practice for pupils 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 also are sent home annually.

Community Use of School ICT Resources

The school's ICT facilities may be used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by C2K. They must also agree to the school's Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

6. Health and Safety

In Donemana 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, which have been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards, Digital Projectors and iPads are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboard, projectors and iPads. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are also mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

Use of Mobile Phones

Many modern mobile phones have internet connectivity. Please refer to the schools Acceptable Use Policy for Mobile Phones and Other Electronic Devices.

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

7. School Website

The school website is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Website reflects the school's ethos that information is accurate and well presented and that personal security is not compromised. The Principal will ensure common values and quality control. As the school's Website 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 Website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website 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 (see Digital Images policy).

- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- 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.

8. Social Software

This is a generic term for community networks, chat rooms, instant messenger (IM) systems, online journals, social networks (Facebook, Twitter, Snapchat, Instagram, etc.) and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.

The majority of activity in these on-line social sites usually causes no concern. C2k filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment.

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. Appropriate information and indeed education will also be provided for our parents.
Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's discipline policy and child protection procedures and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Cyber Bullying can take many forms and guises 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 a 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 – 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.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils will be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
  http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988
  http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003
  http://www.legislation.gov.uk/ukpga/2003/21

We as a school will also keep good records of cyber-bullying incidents to monitor the effectiveness of the preventative activities, and to review and ensure consistency in our investigations, support and sanctions.

Appendix 1

ICT Code of Safe Practice

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.

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. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. 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 G Hay, Donemana Primary School's eSafety coordinator/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 personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware/software without permission of Mrs G Hay.
- 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 inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- 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 my 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.

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

Parental Agreement/Consent Letter

Principal: Mrs G Hay
Address: 31 Longland Road
Donemana
Co. Tyrone
BT 82 0PH

Tel: (028) 7139 8633

Dear Parent/ Carer

As part of Donemana Primary School's Information and Communications Technology programme we offer pupils supervised access to a filtered Internet service provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. 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 G Hay.

✂- -

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 Donemana Primary School.

Parent/ Carer Signature: ……..…………………….…………………………….

Date: ………………………

Appendix 2

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

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails 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.

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	**Accepting** e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.
R	**Remember** 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

eSafety guidelines to be displayed throughout the school

SMILE and 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/ 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.parentcentre.co.uk/category/internet-safety-for-kids 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.