Millquarter Primary School

Online Safety Policy

February 2024

Introduction

Information and Communications Technology (ICT) 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 & Tablets with text, video and/or web functionality

· Other mobile devices with web functionality

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.

In Millquarter Primary School, we understand the responsibility to educate our pupils in Online-Safety issues. We aim to teach the children 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.

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. Key Concerns are:

Potential Contact

Children may encounter 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.

Children should be taught:

· 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 or

· That they should never meet alone anyone contacted via the Internet, and

· That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate 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.

Children should be taught:-

· 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.

Excessive Commercialism

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

Children should be taught:

· Not to fill out forms with a lot of personal details.

· Not to use an adult's credit card number to order online products.

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 Online-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 Online-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 Online-Safety throughout the school.

The Principal and ICT Co-ordinator update Staff and Governors with regard to Online-Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the Online-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 Principal, Staff and approved by the Governing Body. The Online-Safety policy and its implementation will be reviewed annually.

Online-Safety Skills' Development for Staff

· All staff receive regular information and training on Online-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 Online-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 Online-Safety activities and awareness within their lessons.

Online-Safety Information for Parents/Carers

· Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.

· Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.

· The school will communicate relevant Online-Safety information through newsletters and the school website.

Parents should remember that it is important to promote Online-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 & tablets.

· 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.

Teaching and Learning

Internet use:

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

· 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.

E-mail:

· Pupils at this stage will not have access to their e-mail account provided by C2k.

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.

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.

· Staff should not use personal mobile phones during designated teaching sessions.

Managing Video-conferencing:

· Video conferencing will be via the C2k network to ensure quality of service and security.

· Videoconferencing will be appropriately supervised.

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 /will be renewed annually in case there is a change in the child's circumstances where consent could be an issue.

· Parents/carers may withdraw permission, in writing, at any time.

· Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

· Pupils' full names will not be used anywhere particularly in association with photographs outside of school.

· Photographs of individual pupils will be permitted in certain circumstances (Achievement or Reward)

· Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

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 Online-Safety rules. These Online-Safety rules will also 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 Online-Safety rules and within the constraints detailed in the school's Online-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, MIS systems.

Handling Online-Safety Complaints:

· Complaints of Internet misuse will be dealt with by the principal or ICT co-ordinator.

· Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the Online-Safety incident logbook.

· Any complaint about staff misuse must be referred to the Principal.

· Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

· Pupils and parents will be informed of the complaints' procedure.

Communicating the Policy:

Introducing the Online-Safety Policy to pupils

· Online-Safety rules will be displayed in all classrooms 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.

· Pupils will be informed that network and Internet use will be monitored.

Staff and the Online-Safety Policy:

· All staff will be given the School Online-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 is 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 with regard to Internet access, data protection and use of software, both in and out of school.

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.

Signed: _____BoG Chairperson

Signed: _____Principal

Approved by Governors: _____

Next Review: February 2025

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

Millquarter Primary School

Acceptable Use Policy for Foundation Stage Pupils

- I will take care when using the school IT equipment and use it properly.
- I will only share my username and password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will use a safe name and not my real name on the internet.
- I will only take a photograph or video of someone if they say it is alright.
- Any messages I send will be polite.
- I will not deliberately write anything which upsets other people.
- I understand that the school may talk to my parent/guardian if they are worried about my use of school IT equipment.
- I understand that I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if the unacceptable use occurred outside school.

Pupil Name:_____ Class _____

I confirm that I have read and discussed this policy with my child.

Signed

(by adult) _____.

Millquarter Primary School

Acceptable Use Policy for Key Stage One Pupils

- I will look after all the school IT equipment and use it properly.
- I will only share my username and password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I will only take a photograph or video of someone if they say it is alright.
- All of the messages I send will be polite.
- I will not post anything online which upsets other people.
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet.
- I understand that the school may check my use of IT and talk to my parent/guardian if they are worried about my online safety.
- I understand that I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if the unacceptable use occurred outside school.

Pupil Name:_____ Class _____

I confirm that I have read and discussed this policy with my child.

Signed

(by adult) _____.

Millquarter Primary School

Acceptable Use Policy for Key Stage Two Pupils

- I will take care of the school IT equipment and use it responsibly.
- I will keep my password private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images, or messages.
- I will not interfere with anyone else's passwords, settings, or files on the computer.
- I will only use the computer for programs approved by my teacher.
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I know I need permission to take someone's photograph or video them.
- Any messages I post online or send in an email will be polite and responsible.
- I will send or forward messages or create material which is deliberately intended to upset other people.
- I know I must take care about giving away my personal information and contacting people I do not know when using the internet.
- I will not bring any personal devices such as smart watches and mobile phones into school.
- I understand that the school may check my use of IT and talk to my parent/guardian if they are worried about my online safety.
- I understand that I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time, and that this may happen even if the unacceptable activity happened outside school.

Pupil Name:_____ Class _____

I confirm that I have read and discussed this policy with my child.

Signed

(by adult) _____.

The Internet

As part of the curriculum and the development of ICT skills, we provide supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world we live in today.

Although there are concerns about children having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school internet provider C2K operates a filtering system that restricts access to inappropriate materials. All children will be asked to only use the search engine 'Google' when conducting a search in school.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The rules overleaf are displayed in the computer suite and in all the classrooms and children will be reminded of them regularly.

Use of Webcams

A webcam is a camera connected to the internet. Webcams provide a continuous stream of live video, and are typically used for one-to-one conversation, video conferencing or broadcasting across the internet.

Using webcams in the classroom opens up a wide range of teaching and learning possibilities. Webcams can offer teachers effective ways of using ICT across the curriculum which engage children with technology in an interactive way. They allow children to see real time events, bring far-off places to life, and can inspire curiosity and imagination.

Webcams can facilitate collaboration between schools in different parts of the country, or the world, on a joint project. Children will only be using a webcam in school when an adult is present.

Millquarter 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 Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' 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
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- 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
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Name _____

Date Signed _____