St Malachy's Primary School

Online Safety Policy

Acceptable Use of Internet Agreement

Policy Ratified: February 2024

Signed by Principal: Justin Toner

Chair of Governors: Pat O' Hanlon

Introduction

Information and Communications Technology (Using 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 with text, video and/or web functionality
- ✓ Programmable devices (e.g Beebot)
- ✓ Other mobile devices with web functionality

Whilst these UICT 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 St Malachy's Primary School, we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach 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 come into contact with 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.
- ✓ The CEOP 'Click CEOP' button to report concerns.

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. For example, some use the web to publish information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information. For example, 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 online 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 UICT Coordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection). The UICT Coordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The UICT Coordinator will update Senior Leadership and Governors when necessary, with regard to e-safety and all Governors will have an understanding of 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 UICT, Positive Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the UICT Coordinator, Staff, Pupils and Parents and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

E-Safety Procedures for Staff

- ✓ 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.
- ✓ Staff have received information on the issue of 'sexting' from the Department of Education. (Children are not permitted to have their phones in schools). If a member of staff is aware that a child has a phone in school, the child will be asked to hand over the phone which will be left in the safe in the office and their parent will be contacted to come and collect the phone.
- ✓ If a member of staff becomes aware of a child with an inappropriate image, they are to confiscate the device and immediately place it in a sealed envelope. They then report the incident to the teacher responsible for Child Protection who in turn reports it to the PSNI. The sealed device is then locked in a cabinet or safe until collected by the PSNI.
- ✓ New staff members will receive information on the school's Acceptable Use Agreement as part of their induction.
- ✓ Teachers are encouraged to incorporate e-Safety activities and awareness within their lessons and PDMU Curriculum.

E-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 website contains useful information and links to sites like CEOP's thinkuknow.
- ✓ 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 online 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 online may not be who they say they are.

- ✓ Be vigilant. Ensure that children do not arrange to meet someone they meet online.

- ✓ 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.

- ✓ The school will provide e-Safety information on the school website which will be updated by the UICT Coordinator.

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.

C2K defines three types of access;

- ✓ Green – accessible to all users
- ✓ Amber – accessible to school's selected groups of users – includes access to youtube, bbc iplayer etc.
- ✓ Mr Toner will decide on access rights to specific users. (Only Staff)

- ✓ Red – not accessible to any user

No filtering service is 100% effective; therefore, staff members will always aim to supervise pupils use of the internet within the classroom context. Use of the Internet is a planned activity. (Aimless surfing is not encouraged).

- ✓ Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- ✓ 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 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 may only use C2k email accounts on the school system.
- ✓ Staff are asked to only use C2k emails for school business.
- ✓ Pupils must immediately tell a teacher if they receive offensive email.
- ✓ Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

- ✓ The forwarding of chain mail is not permitted.

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 online bullying to the school.
- ✓ School staff are given guidance on their personal use of social media as part of our Staff Acceptable Use 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 are discouraged from using such devices in order to comply with GDPR regulations and ensure no data breaches can occur.
- ✓ Staff should not store pupils' personal data and photographs on memory sticks/iPads or other data storage devices taken outside school.
- ✓ Pupils are not allowed to use personal mobile devices/phones in school.
- ✓ Staff should not use personal mobile phones during designated teaching sessions and when supervising children.

Managing Video-conferencing:

All platforms that bring people together, especially those which mix adults, children and other vulnerable young people have the potential to present a risk. Should the need for video conferencing arise:

- ✓ Video conferencing will be via the C2k network to ensure quality of service and security.
- ✓ Video conferencing will be appropriately supervised.
- ✓ Staff will be reminded to report any Safeguarding concerns at the end of the session.

If Video Conferencing is being used as a home-schooling platform, children will be reminded of the following rules:

- ✓ when they can speak/contribute
- ✓ how they should present themselves on screen (i.e. dressed appropriately)
- ✓ how to interact with others
- ✓ how and when they can leave the 'room'

Seesaw Learning

- ✓ Selected pupils have access to their own Seesaw digital learning journals. Seesaw provides a useful way of collating and celebrating the achievements of our pupils and sharing them with our parents.

- ✓ Pupils are able to post images, videos and audio recordings related to their classwork on their journals.

- ✓ All uploads, including comments, have to be approved by the class teacher.

- ✓ Parents, via the Seesaw Family app and website, only have access to their own child's journal content.

- ✓ Parents are asked to provide consent for their child to use Seesaw when they start St Malachy's Primary School.

Seesaw is compliant with the GDPR in how it stores data. Information link. https://help.seesaw.me/hc/en-us/articles/115005743186-Is-Seesaw-GDPR-compliant-

Publishing Pupils' Images and Work

- ✓ The school seeks parental permission to use children's images, voice or work
- ✓ The school may publish on the school website or in the local newspaper, photographs that will celebrate an individual or group of children's achievements/success.
- ✓ Photographs of pupils are published on the school Website/Newspapers/Other Publications with first name of child only if at all.
- ✓ Parents/carers may withdraw permission, in writing, at any time.

Making and Storing Digital and Video Images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Staff members should use school ipads to take photographs and videos.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

All images will be deleted when they are no longer required.

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 also be displayed clearly in the ICT Suite.

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 UICT resource.

Staff will have different internet access restrictions than pupils. This will allow them to access a greater array of teaching and learning materials. These will be in line with the C2K red, amber and green guidelines.

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 e-Safety Complaints:

- ✓ Complaints of Internet misuse will be dealt with by the Designated teachers and the Principal informed.
- ✓ Deliberate access to inappropriate materials by any user will lead to the incident being logged.
- ✓ 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 safeguarding and child protection procedures.
- ✓ Pupils and parents will be informed of the complaints' procedure.

Cyber Bullying

Cyber Bullying is bullying behaviours that take place over smart phones/mobile phones or the internet. It may include:

- ✓ Hurtful, embarrassing or threatening material posted online (eg. on social network websites)
- ✓ Nasty messages sent as texts, emails or other websites or apps
- ✓ Being excluded from an online game
- ✓ Fake profiles on a social network to make fun of others

Communicating the Policy:

Introducing the e-Safety Policy to pupils

e-Safety rules will be displayed in the UICT 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 and Internet Safety Week.

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

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 is essential.
- ✓ A laptop and iPad 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.
- ✓ Staff will be advised to use social networking sites responsibly and ensure that neither their personal/professional reputation, nor the school's reputation is compromised by inappropriate postings. Staff will be discouraged from being 'friends' with parents on social media.

Monitoring and review:

- ✓ This policy is implemented on a day-to-day basis by all school staff and is monitored by the Principal, Designated Teacher and UICT Coordinator.

- ✓ This policy is the Governors' responsibility and its effectiveness will be reviewed annually.

- ✓ They will do this during reviews conducted between the UICT Coordinator and Designated Teacher for Safeguarding and Child Protection.

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.

St Malachy's Primary School

Acceptable Use of Internet Agreement for Pupils

The school uses computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- ✓ I will access the system with my login and password, which I will keep secret.
- ✓ I will not access other people's files without permission.
- ✓ I will not install or attempt to install any programmes on the computer including Apps on the iPad.
- ✓ I will only use the computers for school work and homework.
- ✓ I will not bring in my mobile phone or other electronic devices into school without permission.
- ✓ I will ask permission from a member of staff before using the Internet.
- ✓ I will only e-mail people I know or those who my teacher has approved.
- ✓ 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 give my home address or telephone number or arrange to meet someone.
- ✓ 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 use Internet chat-rooms or play online games in school that are not allowed.
- ✓ I will never give out personal information or passwords.

Pupil Name: ……

Signed: Parent/Guardian ……

Date: ……

Guidance Material on Internet Safety

http://schoolsl.becta.org.uk **www.ceop.gov.uk** **www.thinkuknow.co.uk**

St Malachy's Primary School

Acceptable Use of Internet Agreement (For Staff)

- ✓ 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 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 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 emails sent and for contacts made that may result in email 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 email 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 is forbidden.
- ✓ All personnel devices brought into school by staff must not have content that could be deemed inoffensive or be misconstrued in any way.
- ✓ Staff may access the school network via their own personal devices in line with this policy for own planning but should use a school designated device for teaching and learning purposes.
- ✓ Any personal information about pupils should not be stored on personal devices – only encrypted devices should be used.
- ✓ Use social networking sites responsibly and ensure that neither your personal/ professional reputation, nor the school's reputation is compromised by inappropriate postings.
- ✓ Do not under any circumstances accept friend requests from a person you believe to be a pupil at your school.
- ✓ It is strongly recommended that Facebook friend requests not be initiated to or accepted from parents.

Signed: ……

Date: ……