St. Mary's Primary School & Nursery Unit, Killyclogher

E-Safety and Acceptable Use of the Internet Policy

Review of Policy	August 2024
Ratification of Policy by the Board of Governors	November 2027
Next Review Date	November 2027

E-Safety and Acceptable Use of the Internet means acting and staying safe when using digital technologies. It is wider than simply internet technology and includes electronic communication via text messages, social environments and apps, and using games consoles through any digital device.

In all cases, in schools and elsewhere, it is a paramount concern.

This Policy is based on and complies with DENI Circular 2013/25, DE Circular 2016.26, DE Circular 2016.27 Online Safety.

The school's E-Safety Policy will operate in conjunction with other safeguarding policies including those for: Positive Behaviour, Anti-Bullying, Child Protection and Safeguarding, Data Protection, Image Consent and Security.

INTRODUCTION

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and promote effective learning. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

RATIONALE

At St Mary's Primary School and Nursery Unit, Killyclogher, we recognise that pupils should have an entitlement to safe internet access. We recognise that this will help our pupils to develop high level ICT skills and prepare them as lifelong learners and for future employment. However, we realise that our E-Safety Policy must provide the necessary safeguards that ensure our pupils are safe and are protected from potential harm, both within and outside school.

This Policy explains how we intend to help children (and their parents / guardians) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Roles and Responsibilities

This Policy helps to ensure safe and appropriate internet use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the Principal and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

Input from staff has been encouraged and incorporated in the review of this Policy. All staff have agreed to follow and implement it. The Policy is circulated to parents/guardians via the school website and via direct school communication methods. The Policy will be reviewed in light of any new guidance and/or every three years.

Scope of the Policy

This Policy applies to all members of the school community - including staff, pupils, parents/guardians, visitors - who have access to, and are users of, the school ICT systems, both in and out of school.

Internet Access

All internet activity should be appropriate to the children's education or staff professional activities;

- Access is limited to the use of authorised accounts and passwords, which should not be shared with others.
- C2k provides every pupil and member of staff with a unique username to access C2k services both within and outside school. Authenticated users are granted access to C2k's filtered internet service. User activity is logged and reports of usage are available to the Principal. Where the school suspects inappropriate use of the internet, the facility to remove access for a user exists.
- The Internet may be accessed by staff and children during their hours in school.
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited.
- It is strongly advised that staff should not use home email accounts for school business and instead use their C2k email system.
- Users are responsible for the content of all email or messages sent by them. Due regard should be paid to language used.
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited.
- The use of the Internet, email or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden.
- Children must not be given unsupervised access to the Internet. For the purposes of this Policy, "supervised" means that the user is within direct sight of a responsible adult.
- Internet access for pupils in schools should be available only on computers that are in highly-used areas of the school such as classrooms, computer suite and resource areas. Computers which are connected to the internet should be in full view of people circulating in the area.
- All pupils in Years 1 through to 7 must sign the child-friendly 'Pupil Acceptable Use of ICT Agreement' at the start of each academic year. (See Appendices (i) and (ii) and (iii)). The Acceptable Use Policy outlines clear rules for the use of equipment within school.
- Parents will be sent a copy of the 'Pupil Acceptable Use of ICT Agreement' which their children will have read with their teachers and signed in class (Appendix (i) and or (ii)).
- Controls on Internet access ensure that access to the internet is regulated for users depending on their role in the school and their age.

Managing Additional Devices

This Policy incorporates the acceptable use of the internet and school-based digital technology and personal mobile technology.

The school uses non-C2K technologies (e.g. iPADs) across all year groups and among staff. These devices are flexible and are used for communication, taking photographs and videos to record pupil activities and achievements which are used for observation and assessment, posted on the school's website or used for display. Such technologies (e.g. iPADs) also give pupils access to educational apps that facilitate development of key skills in technology and across the curriculum. Their flexibility of use allows pupils to carry out research and record and present their learning in a variety of different formats.

These devices access the internet using C2k Meru Wireless. However, it is important to note that the school has an important role in managing internet access with these devices.

- All these devices have the most rigorous restrictions applied to ensure safe internet usage. Age appropriate restrictions are applied to any content that can be accessed and the security of devices used by pupils is reviewed at the beginning of each academic year.

- On these non-C2K devices, as with all internet access, even the most rigorous controls cannot totally eliminate all risk and, therefore, it is necessary to ensure that pupils using them are supervised by a responsible adult at all times.
- All additional technologies that pupils have access to are owned by the school and their safe use can be managed. It is for this reason that pupils are not permitted to bring mobile phones or any personal devices capable of storing or recording digitally into school on any occasion (Please refer to the school's Mobile Devices Policy).

Protecting Pupils

E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology both within and outside the school.

The **Safeguarding Board for Northern Ireland (SBNI) Report (January 2014)** identified four categories of risks facing young people in their use of the internet. The report highlighted the requirement to take appropriate preventative action to protect children and minimise the associated risks.

Content risks: The child or young person is exposed to harmful materials. **Contact risks:** The child or young person participates in adult-initiated online activity and/or is at risk of grooming. **Conduct risks**: The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail. **Commercial risks**: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

To protect pupils from these risks the school ensures:

- Staff avail of Child Protection Training including E-Safety Guidance. Staff are aware of the importance of reporting an incident of concern involving ICT to the school's Designated Teachers for Child Protection and ICT Co-ordinator following the procedures as outlined in the school's Child Protection Policy.
- Staff are aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is recognised as potentially serious and is dealt with within the school's overall Anti -Bullying and Positive Behaviour Policies.
- Care is taken when making use of social media for teaching and learning and activities are risk assessed by staff in the context of each school or home learning situation.
- The school is energetic in teaching pupils how to act responsibly and keep themselves safe in the digital world and, as a result, pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves.

Promoting Internet Safety

The school actively promotes online safety messages for pupils on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety.

As with all other risks, it is impossible to eliminate those risks completely. It is, therefore, essential through good educational provision to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks appropriately.

- The teaching of e-safety is planned and delivered as an age-related online safety curriculum to enable pupils to become safe and responsible users of technology.
- E-Safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT both in and out of school.
- A Safer Internet Day is held annually in school in order to increase awareness of E-Safety.
- Child- friendly rules, linked to the safe use of the internet, are displayed in each classroom and the ICT suite and children are encouraged to know and refer to these SMART rules. These SMART rules are also communicated to parent/guardians through a dedicated Internet Safety section on the school's website.
- Active links to www.thinkyouknow.co.uk and CEOP are posted on the School's website.
- Safer Internet publications and films, including those produced by Child Exploitation and Online Protection (CEOP) and Childnet are used to support the teaching of e-safety for all pupils. Materials from these organisations, to support parents' awareness of internet safety, are annually distributed to parents/guardians and are available to access on the school's website.
- Parents are encouraged to monitor their child's use of the internet ensuring that computers and digital devices have age-appropriate restrictions applied and use internet filters to block malicious websites.
- All children are taught that if they see an unacceptable image, or feel uncomfortable with what is online, they must report this immediately to a responsible adult.
- Pupils are taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information from other sources.
- At St Mary's pupil access to social networking sites including You Tube is blocked on school computers and materials from these sites are only shown to pupils when they have been carefully checked and deemed appropriate by teachers.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils and parents/guardians are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old.

Management of Personal Data

The school ensures personal data is collected and managed responsibly in line with personal data legislation: Data Protection Act 1998, Data Protection Act 2018 and Freedom of Information Act 2000 as outlined in the school's GDPR and Safeguarding Policies.

- At all times care is taken to ensure the safe keeping of personal data (including digital images), minimising the risk of its loss or misuse.
- Personal data is only accessed on secure password protected computers and other devices.
- Staff ensure that they are properly "logged-off" at the end of any session in which they are using personal data.
- Personal details of staff and pupils are securely stored and access is strictly controlled.

Digital Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils' instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and

with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- Staff are allowed to take digital / video images to support educational aims but must follow the school's Child Protection Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Written permission from parents or guardians is obtained at the start of the school year before photographs of pupils are published on the school website or on any other media.

Sanctions for misuse

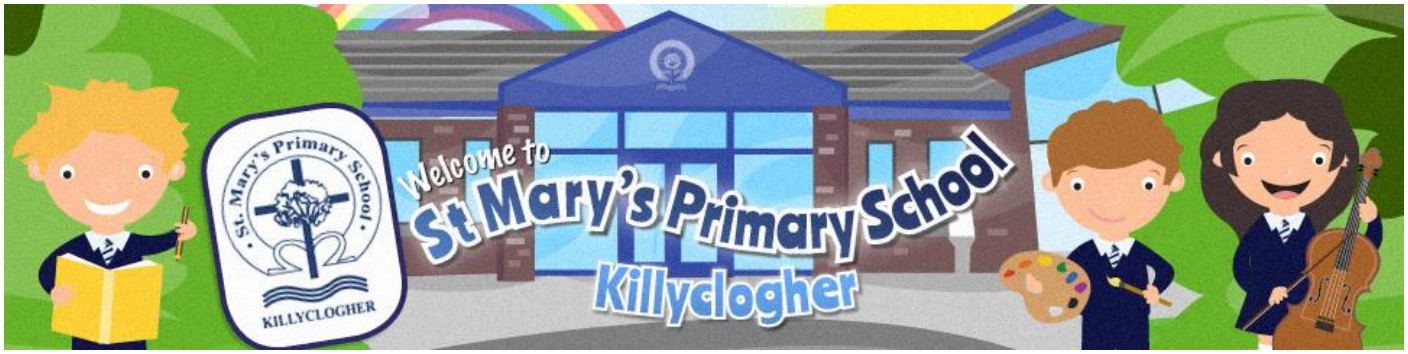
Incidents of technology misuse which arise will be dealt with in accordance with the school's Positive Behaviour and Anti-Bullying Policies. Minor incidents will be dealt with by the Principal/ICT Co-ordinator and may result in a temporary or permanent ban on Internet use.

Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

E-Safety Awareness for Parents

The Internet Safety Policy and Code of Practice for pupils (See Appendix (i) and Appendix (ii)) is sent home annually for parental signature. Internet safety leaflets for parents/guardians are also issued annually. There are also links to internet safety websites on our school website which parents are encouraged to access.

Appendix (i)



Acceptable Use of Internet Policy

Foundation Stage and Key Stage 1

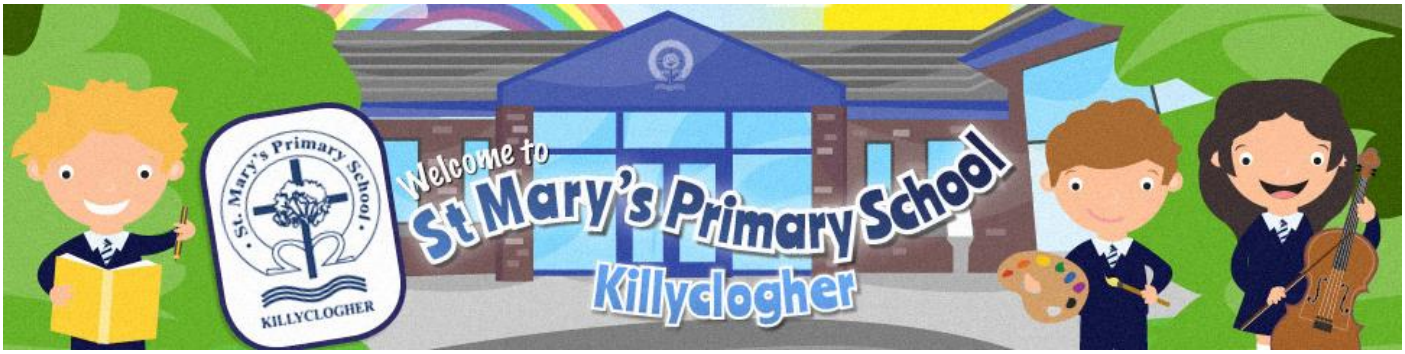
I understand that the St Mary's Primary School Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my password safe.
- I only send messages online which are polite and friendly.
- I know my teachers can see what I am doing online when I use school computers and iPads.
- I always tell a teacher or trusted adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk and www.stmaryskillyclogher.co.uk to learn more about keeping safe online, with the help of my parents/guardians.
- I know that if I do not follow the rules I may not be allowed to use school computers or iPads.
- I have read and talked about these rules with my parents/carers.

Pupil Signature ……

Date ……

Appendix (ii)



Acceptable Use of Internet Policy

Key Stage 2 (7-11)

I understand that the St Mary's Primary School Acceptable Use Policy will help keep me safe and happy online when using ICT in St Mary's and at home.

- I will use the school computers and technology sensibly.
- I will ask permission from an adult before I use the internet.
- I will only log on using my own username and password which I will keep confidential.
- I will only look at my own work and not delete anyone else's files.
- I will not bring in USBs or devices from home without permission.
- I will only email people I know.
- I will always be polite and use appropriate language when emailing or sending messages on the computer.
- I will not give out my personal information or arrange to meet anyone.
- If something on the internet upsets me or makes me feel unhappy or worried, or a stranger sends me a message, I will tell a responsible adult.
- I know school will check my computer and be able to see what I am doing and what sites I have visited.
- If I break these rules I know that I may be stopped from using the internet and/or computers.

Pupil Signature ……

Date ……

Appendix (iii) - Letter issued to parents/guardians

Dear Parent(s)/Guardian(s),

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At St Mary's we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children.

Your child has read the following **Acceptable Use Agreement** in class with their teacher. Your child has signed their name to agree to these points.

Please read these agreements with your child again at home to show your support of the school in this important aspect of our work.
Thank you.

(ICT Co-ordinator)