

St. Mary's Primary School



Acceptable Use of the Internet and Digital Technologies Policy

November 2021

Acceptable Use of the Internet and Digital Technologies Policy

"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."

DENI Circular 2007/1

Introduction

In St. Mary's P.S. we recognise that the Internet and other digital technologies are very powerful resources which can enhance and transform learning and teaching when used effectively and appropriately. The Internet is an essential resource for education, business and social interaction. At St. Mary's P.S. pupils are provided with opportunities to use the Internet, along with helping them develop the skills necessary to access, analyse and evaluate resources available online. This includes educating our children about the potential dangers found on the Internet. Our 'Online Safety Policy' further explains our role in protecting our pupils.

This document sets out the policy and practices for the safe and effective use of the internet in St. Mary's Primary School. The policy has been drawn up by the staff of the school under the leadership of the UICT coordinator and the Principal.

Code of Practice for Safe and Effective Use

When using the Internet, email systems and digital technologies, all users must comply with relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Practice for St. Mary's Primary School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not.

The scope of the Code of Practice covers fixed and mobile Internet, school desktop computers, laptops, iPads and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises or taken on trips (e.g. mobile phones, iPads etc.) are subject to the same requirements as technology provided by the school.

The UICT Co-ordinator will continually monitor the effectiveness of the Code of Practice, particularly in light of new developments in technology.

Code of Practice for Pupils

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

In addition, the following measures have been adopted by St. Mary's P.S. to ensure our pupils' safety when using the Internet and other digital technologies:

- The 'SMART' rules for staying safe online are delivered to pupils at an age appropriate level and displayed prominently in the ICT Suite and in classrooms (Appendices 1A and 1B)
- Our Code of Practice is reviewed regularly and a 'Code of Conduct for using Digital Devices' is signed by parents of pupils from P1-P3 and by both pupils and parents from P4-P7 (Appendices 2A and 2B)
- Pupils using the Internet will normally be working in classrooms where they will be monitored by a teacher or classroom assistant
- All online activity is for appropriate educational purposes
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group, unless engaging in independent research activities
- When undertaking independent research, pupils will be taught to use the keywords 'for children' or 'for kids' to narrow down the search to sites which are age appropriate
- Pupils are not permitted to download apps onto school devices
- The ICT co-ordinator and members of the Senior Management Team may carry out occasional checks on computers, pupil folders and iPads to ensure compliance with this 'Acceptable Use Policy'.
- Pupils are educated in the safe and effective use of the Internet through our preventative curriculum. This includes PDMU, ICT lessons, Anti Bullying Week and Safer Internet Day.

It should be accepted that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

During school hours, pupils are only allowed to play educational computer games/apps specifically assigned by the teacher.

The use of mobile phones by pupils is not permitted on the school premises during school hours. If mobile phones are brought to school, they should be handed in to Mrs O'Kane at the office.

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 Principal and UICT Co-ordinator and may result in a temporary or extended ban on Internet use. Incidents involving Child Protection issues will be dealt with in accordance with school Child Protection procedures.

Code of Practice for staff

The following measures have been adopted by St. Mary's Primary School:

- Pupils accessing the Internet should be supervised by an adult
- All pupils are aware of the rules for the safe and effective use of Digital Devices
- Rules for using Digital Devices will be displayed in the ICT Suite, P3-P7 classrooms and should be discussed with pupils
- All pupils using the Internet have permission from their parents

- Equipment, websites and apps recommended for use by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age appropriate
- Deliberate / accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal / UICT Co-ordinator
- 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. Staff passwords should only be shared by the network manager.
- Teachers should be aware of copyright and intellectual property rights, and should be careful not to download/use any materials which are in breach of these
- Photographs and videos of pupils should, where possible, be taken with school equipment and images should be stored on the secure school network or on the teachers' encrypted pen-drives
- Only approved teaching staff may take photographs and videos of pupils using a personal mobile phone / iPad. These must be deleted as soon as transferred to school network / encrypted pen-drive or uploaded to school approved social media
- Staff will read and sign the Staff User Agreement for Internet Access

Internet Safety Awareness

In St. Mary's Primary School, we believe that alongside having written policies on Online Safety, E-Safety and Acceptable Use of the Internet & Digital Technologies, 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 of the Internet as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

For Pupils

- Pupils take part in age-appropriate Online Safety and Online Communication lessons.
- Rules for e-Safety and use of 'Digital Devices' are discussed with pupils and displayed appropriately.
- 'SMART' rules are discussed with the children and displayed
- All pupils participate in Safer Internet Day each year, completing tasks to reinforce safe use of the Internet
- P7 pupils participate in a transition programme in conjunction with the PSNI which includes information on how to stay safe online
- Digital Leaders ensure that the children have a say in the use of Digital Devices at St. Mary's P.S.

For Staff

- The UICT Co-ordinator is kept informed and updated on issues relating to Internet Safety by regularly accessing specific websites, researching resources and attending relevant courses.
- Information is disseminated to Senior Management, teaching staff and non-teaching staff on a regular basis.
- Staff teach pupils about 'Online Safety' as part of their scheme of work for UICT and create / adopt activities to use as part of Safer Internet Day .

For Parents

- School 'ICT Policy', 'Online Safety', 'e-Safety Policy' and 'Acceptable Use of the Internet and Digital Technologies Policy' are all available to download from the school website or by contacting the school office.
- Links to websites which provide information to parents on how to keep their children safe online are linked within the school website.
- The school provides Internet Safety evenings for parents / carers on an annual basis.

Health and Safety

St. Mary's Primary School attempts, in so far as possible, to ensure a safe working environment for pupils, teachers and ancillary staff when using ICT resources. All staff and pupils are encouraged to take regular breaks from the screen (PC/laptop/iPad) and to use suitable brightness and contrast settings. Pupils are supervised at all times when Interactive Whiteboards and data-projectors are being used.

Digital and Video Images of Pupils

Written parental permission is sought to cover the use of photographs of pupils on the school website, using school social media (Twitter), in the local press and for displays within school.

Staff will ensure that pupils whose parents wish for their child's photograph NOT to be used are withdrawn from all photographs.

School Website

Our school website promotes and provides up to date information about the school, provides information for parents and showcases the work taking place within the classroom. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels / captions
- No pupil is named individually in any photograph
- When pupils are named within a group photo, only Christian names will be given

- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff

Storage of images

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on the school network or school-owned, staff encrypted pen drives, accessible only by staff. Photographs of pupils are removed from computers when they leave the school. From time to time it may be necessary to use personal devices such as a mobile phone to take photographs, i.e. when on a school trip or to upload to the school Twitter feed. This will only be done by approved members of teaching staff. All photos will be transferred to a secure device at the earliest opportunity and then deleted.

Social Software

Chat Rooms, blogs and other social networking sites are blocked at source by C2K. However, we regard the education of pupils in the safe and responsible use of social software as vitally important and this is addressed through Internet Safety lessons and visits from external agencies such as the PSNI. While it is difficult to impose sanctions on what a child does outside of school, instances of cyber-bullying of pupils or staff will be regarded as very serious offences and be dealt with according to the school's Positive Behaviour Policy and Child Protection procedures. Pupils are aware that any misuse of digital technologies within school should be reported to a member of staff immediately.

Mobile Technologies

The use of portable media such as memory sticks and external hard drives will be monitored closely as they could potentially contain viruses or inappropriate material. Staff should only use school provided encrypted pen drives to carry photographs, pupils' personal data and anything else of a 'sensitive' nature off-site.

Pupils are not allowed to use personal mobile devices / phones in school. Staff should not use personal mobile phones during designated teaching hours, unless for the purposes of school business.

Managing Video-conferencing

Video-conferencing will be via the C2K network to ensure quality of service and security, and will be appropriately supervised.

Policy Communication and Parental Agreement

Parents of children in P1- P3 will be given the school's 'Acceptable Use of the Internet and Digital Technologies Policy'. They are asked to complete and return the Code of Practice form on behalf of their child.

Parents of children in P4-P7 are asked to discuss the Code of Practice with their child and both the parent and child should sign and return the form.

Policies and Code of Practice forms will be issued accordingly to new pupils as they join the 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 and Senior Management Team. Due to the ever-changing nature of the Internet and digital technologies, this policy and its effectiveness will be reviewed as required.



P4-P7 (Appendix 1A)

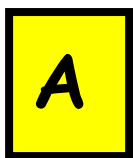
STAY SAFE – FOLLOW THE SMART RULES!



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



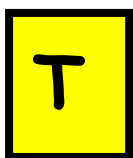
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



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.



STAY SAFE – FOLLOW THE SMART RULES!

S

Secret - Always keep your name, address, and password private.

M

Make sure you tell your parent or teacher if someone wants to talk to you when you are online.

A

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.

R

Remember someone on-line may be telling lies and not be who they say they are.

T

Tell your parent or carer if someone or something makes you feel worried, sad, angry or upset.

P4-P7 (Appendix 2A)



Code of Conduct for Pupils

It is important that all pupils know how to use the Internet responsibly. We request that all pupils read this Code of Conduct which applies every time they use the school computers, laptops or iPads. Parents are also asked to be aware of the Code of Conduct and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password
- I will keep my username and password private
- I will not access other people's files without their permission
- I will not change or delete other people's work / files
- I will ask permission before entering any website, unless my teacher has already approved that site
- I will use the Internet for research and school purposes only
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers / laptops / iPads
- 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 understand that the school may check my computer files / e-mails and may monitor the Internet sites that I visit
- I understand that if I deliberately break these rules I could be stopped from using the Internet / e-mail and my parents / carer will be informed

Signed by Child:

Signed by Parent/Guardian:

Date:

P1-P3 (Appendix 2B)



Code of Conduct for Pupils

It is important that all pupils know how to use the Internet responsibly. We request that all pupils read this Code of Conduct which applies every time they use the school computers, laptops or iPads. Parents are also asked to be aware of the Code of Conduct and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.
- I will keep my username and password private.
- I will not open other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school activities only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand I must look after and take care of the school computer, laptop or iPad I am using.
- 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 understand that the school may check my computer files and may monitor the Internet sites that I visit.
- I understand that if I deliberately break these rules I could be stopped from using the Internet and my parents/carers will be informed.

Name of pupil: _____

Signed by Parent/Guardian: _____
on behalf of child

Date: _____



(Appendix 2C)

Code of Conduct for Staff

The computer system is owned by the school and is made available to all staff to enhance their professional activities including teaching, research, administration and management. The school's 'Acceptable Use of the Internet and Digital Technologies 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 Code of Conduct and return it to the ICT Co-ordinator.

- 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.
- Photographs must be deleted from personal devices once transferred to the secure school folders or forwarded to relevant staff for use on approved school social media.

Name	
-------------	--

Date		Signed
-------------	--	---------------