Digital Safety & Acceptable Use Policy

St Mary’s Primary School
Banbridge

(Updated 2022)

Rationale

"*The school's actions on and governance of online safety must be reflected clearly within the school's safeguarding arrangements and* Online Safety Policy*. Safeguarding and promoting pupils' welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities*."
DENI Online Safety Guidance, Circular number 2016/27

It is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Digital Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The school must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The Digital Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/ guardians) to be responsible users and stay safe while using the Internet and other communication technologies for educational, personal and recreational use.

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. The Internet technologies children and young people are currently using, both inside and outside of the classroom, include:

- Websites/ Apps
- 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
- 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 St Mary’s Primary School we understand the responsibility to educate our pupils about digital safety issues. We aim to teach them 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.

What is Digital Safety?

Digital safety is about using digital devices in a smart but safe way. It means educating children and young people to act responsibly and keep themselves safe in the digital world. It highlights the responsibility of the school, all Staff, Governors and parents to mitigate risk through reasonable planning and actions. Digital Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

Within St Mary’s PS, Digital Safety:

- □is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

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 and is an integral part of pupils' lives, both inside and outside school. 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 and potential risks for the school can be categorised as the Content, Contact and Conduct of activity.

1. Content

- Access to illegal, harmful or inappropriate images or other content.
- Access to unsuitable video/ online games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.

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, use of drugs etc.

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.

2. Contact

- Inappropriate communication/ contact with others, including strangers.
- The risk of being subject to grooming by those with whom they may make contract on the Internet.
- Cyber-bullying.
- Unauthorised access to/ loss of/ sharing of personal information.

Potential Contact

Children may come into contact with someone online who may wish to harm them. Some adults use social networks, chat rooms, e-mail or online games 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 people they encounter through the Internet.
- That they should never give out personal details.
- That they should never arrange to meet anyone contacted via the Internet.
- That once they publish information it can be disseminated with ease and cannot be destroyed.

3. Conduct

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The sharing/ distribution of personal images without an individual's consent or knowledge.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive or potentially inappropriate. Websites may also expose them to marketing schemes or hidden costs/ fraud.

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 appropriately online and understand the importance of discussing problems or issues that may arise. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

As Digital 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. The ICT Coordinator has responsibility for leading and monitoring the implementation of Digital Safety throughout the school and keeps abreast of current Digital Safety issues and guidance through relevant organisations such as NSPCC, CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Coordinator will ensure that all staff are aware of the procedures that need to be followed in the event of a Digital Safety incident taking place and provide training and advice for staff. The ICT Coordinator and Principal will also liaise with C2K, EA and DENI regarding any Digital Safety developments. The Principal/ ICT Coordinator update Senior Management and Governors with regard to Digital Safety and all Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Designated/ Deputy Designated Child Protection Teacher

The Designated Child Protection Teacher/ Deputy Designated Child Protection Teacher will be trained in Digital Safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Managing the Network

The ICT Coordinator will monitor that C2k Online Safety measures, as recommended by DENI, are working efficiently within the school. They will ensure that:

- C2k/ BT system operates with robust filtering and security software.
- monitoring reports of the use of C2k/ BT are available on request.
- school infrastructure and individual workstations are protected by up to date virus software.
- school meets required Digital Safety technical requirements.
- users may only access the networks and devices through use of individual passwords which are regularly changed.
- the filtering policy is applied and that its implementation is not the sole responsibility of any single person.
- they keep up to date with Digital Safety technical information in order to effectively carry out their Digital Safety role and to inform and update others as relevant.
- software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- the “administrator” passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place.

Digital Safety Skill Development for Staff

- All staff receive regular information and training on Digital Safety issues from the ICT Coordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Digital 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 Digital Safety activities and awareness within their lessons.

Digital Safety Information for Parents/ Guardians

- Parents/ guardians are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/ guardians 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 Digital Safety information through Newsletters, App and the school website.

Parents/ guardians should remember that it is important to promote Digital 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 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 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.

CCTV

The school has CCTV as part of our site surveillance for staff and student safety. Access to and disclosure of images recorded by CCTV is restricted. This ensures the rights of individuals are retained.

Teaching and Learning

- The school will plan and provide opportunities within a range of curriculum areas to teach Digital 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 Digital 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/ guardian, teacher/trusted member of staff, or an organisation such as Childline/ CEOP/ NSPCC.
- The school Internet access is filtered through two systems including the C2K managed service and Draytek (Classnet).
- 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 Digital Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. Our School Mascot Ping displays **SMART** tips around the school. These are also discussed and displayed in class.
- Safer Internet Day is celebrated annually in February when children are reminded of important safety messages.

Email

- Pupils may only use C2k email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual email addresses. In some instances children may have access to a group email address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

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 may 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.
- Further information is provided to staff during in service training.
- 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. If necessary, these must be password protected.
- **Pupils are not allowed to use personal mobile devices/ phones in school. Mobile phones brought to school by children will be confiscated. Parents will be required to collect the phone from the school office.**
- Staff should not use personal mobile phones during designated teaching sessions nor should they be used to photograph children in school or a school related activity.

Managing Video Conferencing

- Video conferencing will be via the C2k network (Collaborate/ Microsoft Teams) to ensure quality of service and security.
- Video conferencing will be appropriately supervised.

Publishing Pupils' Images and Work

- Written permission from parents/ guardians will be obtained before photographs of pupils are published. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/ guardians 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 should not be used on the school website, particularly in association with photographs.
- Photographs of individual pupils will be limited. Group pictures will be encouraged.
- Pupil's work can only be published by outside agencies with the permission of the parents/ guardians.

The Data Protection Act

The school is GDRP compliant. St Mary's PS has an updated GDPR Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media, it is advisable that:

- the device is password protected
- the device offers approved virus and malware checking software

- the data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete

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 Digital Safety rules. **These Digital 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 Digital Safety rules and within the constraints detailed in the school's Digital 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,

Handling Digital Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Coordinator and recorded in the Digital 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.

Cyber-Bullying

Cyber- bullying can take many different forms and guises including:

- Email- nasty or abusive emails which may include viruses or inappropriate content.
- Messaging Apps and Forums- 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.

Incidents of cyber–bullying will be dealt with in accordance with the St Mary's PS Child Protection Policy and Anti-Bullying Policy.

Communicating the Policy

Introducing the Digital Safety Policy to Pupils

- Digital Safety rules will be displayed in all classrooms and Ping (school mascot) will share SMART tips. These are discussed with the pupils at the start of each year and regularly reinforced. 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/ Safer Internet Day.
- Pupils will be informed that network and Internet use will be monitored**.**

Staff and the Digital Safety Policy

- All staff will be given the Digital Safety Policy and its importance will be 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/ 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.

Monitoring and Review

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 should be read in conjunction with other school policies including ICT Policy, GDPR Policy, CCTV Policy, Positive Behaviour Policy, Health and Safety Policy, Child Protection Policy and Anti Bullying Policy.

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Coordinator. It has been agreed by the Senior Management Team, Staff and approved by the Governing Body.

This Policy and its implementation will be reviewed annually.

Safety Rules for Children

Follow these SMART tips:

Childnet International

BE SMART ONLINE

S — SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M — MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

THINK U KNOW .CO.UK

A — ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R — RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T — TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**

BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

WWW.CHILDNET.COM

St Mary’s Primary School

Acceptable Use Agreement for Pupils and Parents

Children should know that they are responsible for their use of the Internet and digital technology in school and that they must use it in a safe and appropriate manner. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I understand that the school will monitor my use of the Internet, email and other digital communication.
- I will use the Internet for research and school purposes only.
- I will not share my passwords nor use any other person’s username and password.
- When sending email, I will not give my name, address or phone number or arrange to meet anyone.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I recognise the importance of treating others with respect and will be polite and responsible when I communicate with others.
- I will not use offensive, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will never participate in any sort of online bullying.
- I will respect the work and property of others and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will not take or distribute images of anyone without their permission.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will only open email attachments if I know and trust the person who sent the email.
- I understand that mobile phones are not permitted for use on school premises or at school related activities.
- I will not try to upload, download or access any materials which are illegal or inappropriate or

may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials.

- I understand that if I deliberately break these rules I could be stopped from using the Internet/ email and my parents/ guardians will be informed.

……………………………………………………………………………………………………

Acceptable Use Agreement for Pupils

Please complete and return to your child's class teacher.

As a school user of the Internet, I agree to follow the school rules on its use. I will use the Internet and digital technologies in a responsible way and observe all the restrictions explained to me by my school.	
Pupil Name: *(print)*	Class:
Pupil Signature:	Date:
As the parent/ guardian of the pupil above, I give permission for my child to use the Internet, including email. I understand that pupils will be held accountable for their own actions. I also accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information.	
Parent Name: *(print)*	
Parent Signature:	Date:

St Mary’s Primary School

Acceptable Use 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 Digital Safety and Acceptable Use Policy has been drawn up to protect all parties and ensure staff are aware of their professional responsibilities when using any form of ICT. Staff are expected to sign this Acceptable Use Agreement and adhere to its contents at all times. 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.

- All Internet activity and use of digital technologies 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.
- Personal details such as mobile phone number, personal email address or social media accounts should never be shared with pupils.
- Activity that threatens the integrity of the school ICT systems or attacks/ corrupts other systems is forbidden.
- Software or hardware should not be installed without permission from the ICT Coordinators.
- Users are responsible for all email sent and for contacts made that may result in email being received.
- Attachments should only be opened from sources known to be safe.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language/ content should be applied as for letters or other media.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Personal data must be kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely.

- Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop, iPad or memory stick.
- Use of the network to access, upload or distribute inappropriate materials that could be considered offensive, illegal or discriminatory is forbidden.
- Images of pupils/ and or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent/ guardian or staff member.
- Online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- Pupil safety and responsible use of digital technologies should be supported in accordance with the school's Digtial Safety and Acceptable Use Policy.

……………………………………………………………………………………………...

I agree to follow this Acceptable Use Agreement and to support the safe use of ICT throughout the school.

Name: ______________________________________ Date: ___________________

Signature: ____________________________________

Staff should sign a copy of this Acceptable Internet Use Agreement and return it to the ICT Coordinators.