St. Mary's Primary and Nursery Unit

e-Safety Policy

Updated 19th September 2020

We are a Rights Respecting School. The articles from the UNCRC are an integral part of our UICT Policy.

Article 19

You have the right to be protected from being hurt or badly treated.

Article 28

You have the right to education.

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools:

"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 2007/01

Rationale

The Boards of Governors has a duty to:

-safeguard and promote the welfare of pupils; and
(Article 17 of the Education and Libraries (Northern Ireland) Order 2003).

-determine the measures to be taken at a school to protect pupils from abuse
(*Article 18 of the Education and Libraries (Northern Ireland) Order 2003).*

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The school has a duty of care to enable pupils to use on-line systems safely. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. It covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

This policy should be read alongside the following school policies: Pastoral Care Policy, Positive Behaviour Policy, Safeguarding Child Protection Policy, Anti Bullying Policy, Health and Safety Policy, Seesaw Policy and the ICT Policy.

Introduction

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in St. Mary's Primary School and Nursery Unit and is brought to the attention of all stakeholders. This policy has been drawn up by the staff of the school under the leadership of the ICT co-ordinator. This policy and its implementation will be reviewed bi-annually or sooner where necessary.

We aim to develop mature systems of e-Safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies. As new technologies are developed, the school will respond quickly to any potential e-Safety threats posed by their use.
This policy is largely based on:

- *DENI Circular 2007/1 'Acceptable Use of the Internet and Digital Technologies in Schools'*
- *DENI Circular 2011/22 'e-Safety Guidance'*
- *DENI Circular 2016/26 'Effective Educational Uses of Mobile Digital Devices'*
- *DENI Circular 2016/27 'Online Safety'*
- *DENI Circular 2017/04 'Safeguarding and Child protection: A Guide for Schools'*

The policy should also be read in conjunction with the School's Safeguarding policies.

What is e-Safety?

E-Safety (electronic safety) in the school context:

*is concerned with safeguarding children in the digital world, with an emphasis on learning to understand and use 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.

ICT is a compulsory cross-curricular element of the NI Curriculum and the school must ensure acquisition and development by pupils of these skills. The Internet and digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The school provides pupils with opportunities to use the excellent resources, along with developing the skills necessary to access, analyse and evaluate them.

e-Safety Coordinator

The e-Safety Coordinator, *Mrs McWilliams,* will lead e-Safety in school and takes day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school's policies/documents.

The e-Safety Co-ordinator will:

• Ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.

• Provide training and advice for staff

• Liaise with C2K and school ICT technical staff

• Liaise with the EA and DENI on e-Safety developments

• Receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments.

• Meet regularly with Principal to investigate/monitor abuse of social network sites by pupils.

• Attend relevant meetings with Board of Governors

• Discuss current issues, review incident logs

• Monitor and report to staff any risks to staff of which the e-Safety co-ordinator is aware

• Find out about, discuss with staff and oversee the process of the 360 Degree Safe Review Tool.
•Liaise with Digital Leaders to help promote the message of e-Safety in St. Mary's PS and NU

The Child Protection Officer

The Child Protection Officer, *Mrs McWilliams*, and deputies, *Mrs Fegan and Mrs F McGill*, will be trained in e-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

The Principal

The Principal, *Mrs M. McCann*, has a duty of care for ensuring the safety (including e-safety) of members of the School and Nursery community though the day-to-day responsibility for e-safety will be delegated to the e-Safety co-ordinator.
The Principal will be kept informed about e-safety incidents.
The Principal will deal with any serious e-safety allegation being made against a member of staff.
The Principal and SLT are responsible for ensuring that the e-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-Safety incidents and monitoring reports. The e-Safety policy will be shared with and ratified by the Board of Governors on an annual basis.

Network Managers – *Mrs C McWilliams and Mrs M. McCann*

The Network Managers will monitor that C2K e-safety measures, as recommended by DENI, working efficiently within the school to ensure that:

• The C2k system operates with robust filtering and security software

• Monitoring reports of the use of C2k are available on request by the Principal.

• The school infrastructure and individual workstations are protected by up to date virus software.

• The school meets required e-safety technical requirements.

• That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

• The filtering policy from C2k is applied and that teachers have a duty to report any inappropriate material through the reporting form. (See Appendix 6)

• That they keep up to date with e-Safety technical information in order to effectively carry out their e-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 are available to the Principal and kept in a secure place .

Teaching and Support Staff

Teachers are the first line of defence in e-Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. e-Safety training is therefore an essential element of our staff induction. Through our e-Safety policy, the school can ensure that all reasonable actions are taken and measures put in place to protect all users.
e-Safety training is linked with Safeguarding Training. Safeguarding training is delivered annually to all staff. The induction programme for new staff includes e-Safety. The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff and classroom assistants are made aware of the Department's guidance and advice on ICT use in teaching and learning and are updated in relation to relevant changes.

The Child Exploitation and Online Protection Centre (CEOP) run regular one-day courses for teachers in Northern Ireland. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with www.thinkuknow.co.uk.

The Teaching and Support Staff are responsible for ensuring that:

• They have an up-to-date awareness of e-safety matters and of the current school e-Safety policy and practices.

• They have read, understood and signed the school's ICT Code of Safe Practice for Staff. (See Appendix 3)

• They follow the school e-Safety Policy and ICT Code of Safe Practice.

• They report any suspected misuse or problem to the e-Safety Co-ordinator.

• Digital communications with students (email / Virtual Learning Environment -VLE) should be on a professional level only carried out using official school systems (c2k). Emails should be sent in accordance with the school's Code of Safe Practice.

• e-Safety issues are embedded in all aspects of the curriculum and other school activities.

• Pupils have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act (1998)

• They monitor ICT activity in lessons, extracurricular school activities.

• They follow the ICT Scheme of Work, to include discreet lessons on e-Safety.

• They display the e-Safety Code of Conduct Agreement and 'Be SMART, Be Safe' poster. (See Appendices 1 and 2)

Professional Development for Teaching and Support Staff

Training will be offered as follows:

•All new staff will receive e-safety training as part of their Induction Programme, ensuring that they fully understand, agree to and sign the school e-safety policy and ICT Code of Safe Practice.

•A programme of e-safety training will be made available to staff as an integral element of CPD. Training in e-safety will be supported within the PRSD or EPD process and where staff have identified a need.

•Staff will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

•This e-safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

Pupils

Are responsible for ensuring that:

•They use the school ICT systems in accordance with the ICT e-Safety Code of Conduct Agreement (See Appendix 1), which they will be expected to sign each academic year before being given access to schools systems.

•They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.

•They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. (See appendix 6)

•They know and understand school policies on the taking / use of images and on cyber-bullying.

•Pupils are introduced to email and taught about the safety and 'netiquette' of using e-mail both in school and at home.

•They understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety Policy covers their actions out of school, if related to their membership of the school.

e-Safety Education for Pupils

We believe that, alongside a written e-Safety Policy and ICT eSafety Code of Conduct Agreement, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication, both inside school and outside school. We see education as appropriate, effective and an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

e-Safety education takes place through both discrete lessons and wider curriculum lessons. ICT Agreement Rules, which have been drawn up with the help of pupils are discussed and are prominently displayed in all classrooms. Pupils are made aware of copyright and plagiarism. Pupils are encouraged to validate the accuracy of information which they research.

e-Safety education for pupils will be provided in the following ways:

•e-safety will be provided as part of their lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources as well as other resources will be used as a teaching tool.

•Pupils will be taught in all relevant lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.

•Pupils will be helped to understand the need for the e-Safety Rules and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

•Where pupils are allowed to search the internet, they should only use the 'google' search engine and staff should be vigilant in monitoring the content of the websites pupils visit.

• Important messages will be delivered through PDMU preventative curriculum assemblies on Friday mornings e.g. cyberbullying, Being SMART, Ways to keep safe online.

• Pupils will participate in Internet Safety Week in February and take part in activities associated with the annual event.

• Pupils will participate in the BEE SAFE programme in May.

Whilst the current situation of Covid 19 is changing on an almost daily basis, we strive to continue to deliver e-Safety messages in other innovative ways.

Parents/ Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the e-Safety policy outlined by the School.
Parents and carers will be asked to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

•digital and video images taken at school events

•online communication with staff

•their children's personal devices in the school

(See Mobile Digital Devices Policy)

Parents/ Carers Training and Support

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The e-Safety Code of Conduct Agreement (Appendix 1) and Parent consent form are sent home at the start of each school year for discussion with their child and parents sign and return to school. The e-Safety Policy is sent home annually to parents and it, along with other e-Safety materials are available on the school website. Internet safety leaflets for parents and carers are sent home annually in February. Parents/carers' attention is drawn to the school website and school newsletter where e-Safety messages are provided.

The School will seek to provide information and awareness to parents and carers through:

•The school website www.stmaryspsbellaghy.co.uk provides links to external sites such as CEOP and Digital Parenting

• Policies and e-Safety rules are sent home at the beginning of each academic year. Parents are asked to return the consent forms for internet access for their child at school and also that they will encourage and model responsible internet use at home.

•Letters, newsletters, websites and other information leaflets will be distributed.

•e-Safety Guidance will delivered through key events.

• Internet Safety Week will be highlighted annually and PSNI are invited in to speak during this week.

• Parents are informed of the school's complaints policy which is on the school website. Parents are also informed on how to report issues to the school.

Internet Services

Connectivity and Filtering

The school has one internet systems in its infrastructure. Internet access is filtered for all users.

1. C2K

Classroom 2000 (C2k) is responsible for the provision of the ICT managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.
Internet use is monitored. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting concerns about the filtering system, (See Appendix 6.) Where personal devices are allowed, c2K filtering will be applied that is consistent with school practice.

Some of the safety services include:

• Providing all users with unique user names and passwords

• Tracking and recording all online activity using the unique user names and passwords

• Scanning all C2k email and attachments for inappropriate content and viruses

• Filters access to web sites

Auditing and Reporting

Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school's filtering policy is held with The Principal and the ICT Coordinator.

They manage the school filtering by:

• Monitoring reports of the use of C2k which are available on request.

• Keep records and logs of changes and of breaches of the filtering systems.

• Keeping up to date with the latest guidance regarding filtering services.

Staff and children have a responsibility to report immediately to the e-Safety Coordinator any infringements of the school's policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Code of Safe Practice

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. Staff and pupils are made aware that use of the school's ICT resources is a privilege which can be removed.
The school has:
(a) a Pupil Code of Practice called e-Safety Code of Conduct Agreement (Appendix 1); and

(b) an ICT Code of Safe Practice for Staff (Appendix 3)

Both the above documents make it explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, 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 (such as mobile phones, camera phones) is subject to the same requirements as technology provided by the school.
Mrs McWilliams, the ICT Co-ordinator and the Principal will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology and amend as necessary.

Code of Safe Practice for Pupils

A parental/carer consent letter accompanied by the e-Safety Code of Conduct Agreement for pupils (Appendix 1), is issued to parents/carers at the beginning of the new school year. This consent must be obtained before the pupil accesses the internet.
The following key measures have been adopted to ensure pupils do not access any inappropriate material:

• The school's e Safety Code of Practice for Use of the Internet and other digital technologies is made explicit to all pupils;

• e-Safety guidelines are displayed prominently throughout the school.

• Pupils and their parents/carers are asked to sign the e-Safety Rules.

• Pupils, using the Internet, will normally be working in highly-visible areas of the school;

• All online activity is for appropriate educational purposes and supervised, where possible;

• Pupils will, wherever possible, use sites pre-selected by the teacher and appropriate to age group;

• Pupils are educated in the safe and effective use of the Internet, through a number of selected websites, including CEOPS and Thinkuknow.

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school or C2K can accept liability under such circumstances.

Code of Safe Practice for Staff

It is vital that staff adhere to the *GTCNI Code of Values and Professional Practice*. Staff have access to computers, iPad, email, VLE and Internet access to assist them in the performance of their work. Staff should have no expectation of privacy in anything they create, store, send or receive using the school computer equipment. The computer/iPad network is the property of the school and may only be used for school purposes. The school reserves the right to access activity and staff/pupils should be aware that improper use can lead to disciplinary action.
The ICT Code of Safe Practice has been agreed with staff. (See Appendix 3).
Pupils accessing the Internet should on the whole be supervised by an adult at all times. Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils. Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to Mrs McWilliams.

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. Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these. Photographs of pupils should be taken with school equipment and images stored on the staff folder or an external school storage device, accessible only to staff or under supervision for pupil work.

School systems may not be used for unauthorised commercial transactions. Staff are expected to have secure passwords which are not shared and changed periodically. A Staff Safe Code of Conduct is signed by all staff for each academic year.

Staff will ensure that any posts or messages they put up on Seesaw are appropriate.

Health and Safety

We have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and the ICT suite where pupils are supervised at all times. Guidance is issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. The school considers all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use. In so doing, pupils are informed of what to do if they come across inappropriate material or situations online. (see appendix 4)

Use of Mobile Phones

As agreed in the pupil e-Safety Code of Conduct Agreement, pupils are discouraged from bringing a mobile phone to school. Should a child come to school with a mobile phone, it will be collected by the class teacher and kept for safe keeping throughout the day. If children need to contact a parent during the school day, they can inform their teacher who will assist them to access to the school landline. Should a child bring a phone to school and use it inappropriately, it will be collected and kept in the school office for safe keeping. Parent will be informed and will be required to collect the phone from the school office in person. The Principal will deal with this issue in accordance to the schools Mobile Phone Policy.

Digital and Video Images

Parental permission is gained when publishing personal images on the website, on See Saw or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached). The school gains parental/carer permission for use of photographs or video images. Staff are allowed to take images to support educational aims. Staff must follow school policies concerning the distribution and publication of photos. Pupil names associated with images will not be shared on the school website. Digital images are securely stored centrally on the staff folder or on the school's external storage device and disposed of in accordance with the Data Protection Act.

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available on The Health Protection Agency website.

Personal Data

The school ensures all staff know and understand their obligations under the Personal Protection Act and comply with these to ensure the safe keeping of personal data, minimising the risk of loss or misuse of personal data. Staff have enhanced password protection with at least one capital letter and one number.

Data Protection Act

Staff are regularly reminded of the Data Protection Act.

In particular staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss and nature
- Ensure they are properly logged off at the end of a session and devices are password protected
- Transfer personal data using encryption and secure password protected devices
- Data is securely deleted from the device, in line with school policy, once it has been transferred or its use complete.

Social Media

Whilst social media is not used by St. Mary's at present, we still consider it our responsibility to teach our pupils how to keep safe online as we are aware a number of our pupils have social media accounts or access to social media. We advise on the restricted age limit for each programme and ways on how to keep safe when using them. This information is displayed in the computer suite and is also distributed to parents so they have a full understanding of the implications that social media can have. Friday morning, PDMU assemblies also highlight the potential dangers associated with social media if not properly used.

Cyber Bullying

Staff are made 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 considered within the schools overall Anti-Bullying policy and Pastoral Care Policy as well as the e-Safety Policy. During Friday assemblies, PDMU messages are discussed and children are regularly reminded of what cyber bullying is, how it affects others and what to do if they are being bullied online. Children are regularly reminded of who the Designated and Deputy Designated teachers for Child Protection are.

Cyber Bullying can take many different forms and guises including:

• Email – nasty or abusive emails which may include viruses or inappropriate content.

• Instant Messaging (IM) and Chat Rooms – 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 occurs 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.

• Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils will be reminded that cyber-bullying can constitute a criminal offence.

Pupils are encouraged to report incidents of cyber-bullying to their parents and the school. (See Appendix 4.) If appropriate, the PSNI may be informed to ensure the matter is properly addressed. The school will keep records of cyber-bullying incidents to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

School Website

The school website www.stmaryspsbellaghy.co.uk is used to celebrate pupils' work, promote the school and provide information to parents and the community. The website reflects the school's ethos. Information is accurate and well-presented and personal security is not compromised.

The following rules apply:

•The point of contact on the website is the school address, school info e-mail account and telephone number.

•Staff or pupils' home information will not be published.

•Website photographs that include pupils will be selected carefully by each class teacher. Photographs of children whose parents have not given permission for their use beyond the school environment are not used.

•Pupils' full names will not be used in association with photographs.

•The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Actions and Sanctions for Reporting and Misuse

Pupil Incidents

We believe that it is important that the school has a culture under which users understand and accept the need for e-safety regulations and adopt positive behaviours, rather than one in which attitudes are determined solely by sanctions.

Reporting Pupil Incidents

Users will understand their responsibilities to report e-safety incidents. They will know and understand that there are clear systems for reporting concerns and understand who they can talk to. (See Appendix 4.)

Incident reports will be logged for future auditing, monitoring, analysis and for identifying serious issues or patterns of incidents. This will allow the school to review and update e-Safety policy and practices.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Steps to follow with pupil incidents

1. In the first instance, issues should be reported to and documented by Mrs McWilliams (ICT and e-Safety Co-ordinator and Designated Teacher for Child Protection)
2. The issue should be relayed to the Principal (Mrs M. McCann)
3. Minor issues will be dealt with by Mrs McWilliams according to the school's Behaviour Policy.
4. More serious issues will be dealt with by the Principal who will involve whatever outside agencies deemed necessary.

Sanctions for Pupils Incidents

Minor school related incidents will be dealt with by Mrs McWilliams. This may result in parents being informed, a temporary ban on Internet or device use and/or a loss of Golden Time. Incidents of technology misuse which arise will be dealt with in accordance with the school's Behaviour Policy. This may involve the pupil being supervised 1-1 for an agreed period following a breach of e-Safety rules. Parents will be informed of breaches of contract and /or failure to handle devices carefully.

Incidents Involving Child Protection Issues

Incidents involving child protection issues will be dealt with in accordance with the school's *Safe Guarding and Child Protection Policy*. Parents and where necessary, PSNI, Social Services, Governors will be informed.

Staff Incidents and Reporting

All new staff, volunteers and students on work experience are provided with an induction programme. This includes child protection, ICT Code of Safe Conduct for staff and e-Safety Code of Conduct Agreement for pupils.

The ICT Code of Safe Conduct is signed by all staff on an annual basis. The school's e-safety policy is reviewed biannually.

Any breach of the ICT Code of Safe Conduct for Staff or e-safety Rules will be dealt with by the principal and/or governors.

Staff Sanctions

Governors will deal with breaches of policy by the staff.
Governors will refer to the DE Governor's Handbook
Governors will take advice from appropriate authorities.

Governors will follow the EA Disciplinary Guidelines.

Monitoring and Self Evaluation

The school's wider self-evaluation processes address e-safety in the overall ICT and Safeguarding Child Protection Policy reviews. All key stakeholders are part of the self-evaluative review and participate in questionnaires and surveys. Pupils offer a voice through Digital Leaders and school council meetings. St. Mary's PS, ICT co-ordinator has used The 360 Degree Self-Evaluative Review Toolkit to enable the school to identify areas of need regarding the teaching and learning of e-Safety and address these issues with clear action. The findings will be shared with staff 2019-2020. Monitoring records of e-safety incidents are presented to the Governors.

This policy will be reviewed and amended in light of evidence provided by monitoring, updated technologies or new DE Guidance.

_____ *Chair of BOG*

This policy will be reviewed in September 2021 or sooner due to new guidance.

Appendices

Appendix 1

‘e-Safety Code of Conduct’ Agreement

2020-2021

These rules will keep **everyone safe** and **help us be fair to others.**

- I will ask permission before using the Internet.
- I will only use my **own network login** and **password.**
- I will only look at or delete my own files.
- I will only e-mail people my teacher has approved.
- I will not open an email from someone I do not know.
- I will immediately close any webpage I am not sure about and tell an adult.
- The messages I send will be polite and sensible.
- I will only upload and post appropriate pictures, photographs, work and videos on Seesaw.
- I understand my class teacher will approve each of my posts before it is live on Seesaw.
- I understand that I must never give out personal information or arrange to meet someone I do not know.
- I can only use websites my teacher has chosen or the search engine **‘Google’** when conducting a search at school.
- I will not use Internet chatrooms or any social media sites.
- If I see anything I am unhappy with or if I receive messages I do not like, **I will tell a teacher immediately.**
- I understand that the school may check my computer files and the Internet sites I visit.
- I will only use the webcam when supervised by an adult.
- I will not bring personal ICT equipment into school or on school trips, including mobile phones, tablets and personal cameras. If these are brought into school, it will be dealt with in accordance with the School Mobile Digital Device Policy.
- I understand that if I deliberately break these rules, I will not be allowed to use the Internet or computers for an agreed amount of time.

DECLARATION

We have discussed the information in the St. Mary’s ‘e-Safety Code of Conduct’ Agreement

(child’s name)…… Class ……. agrees to follow the e-Safety Code of Conduct and to support the safe use of ICT at St. Mary’s Primary School and Nursery Unit.

Pupil Signature: _____ Date : _____

Parent/Carer Signature: _____ Date: _____

Appendix 2

Be SMART, Be Safe!

S Keep Safe...

Never tell someone on the internet or on a mobile phone your full name, your address or your telephone number.

M Never Meet...

Never meet up with an online friend. If somebody asks to meet you, tell an adult. **Never** go alone.

A Never Accept...

Never accept emails or text messages from people you do not know.

R Reliable...

Never rely on what you see on the internet. It's not always true. Don't rely on people you meet online they may lie about who they are.

T Always Tell...

Always tell an adult if somebody upsets you. Tell and adult if you see something on the computer that makes you sad.

Appendix 3

ICT Code of Safe Practice and Data Protection Statement for Staff 2020-2021

"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 2007/01

UNCRC Article 29
'Every child has the right to an education. This education must nurture a child's respect for themselves, others and their environment.'

ICT (including data) and the related technologies such as e-mail, internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs C McWilliams (ICT and e-Safety Coordinator) or Mrs M. McCann (Principal).

EMAIL AND SEESAW: I will only use my school email, class Seesaw, internet, learning platforms or any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors. I will use the approved C2k secure e-mail system for school business and communication with parents. I will ensure that all electronic communications with pupils and staff are compatible with my professional role. I will not install my personal email account on the mail app on the iPad but it can be accessed through Safari. I will be careful when opening attachments as they may be infected with a virus. I will take care when using Seesaw to post appropriately using the class journal and private inbox.

PASSWORDS: I will comply with the C2K ICT system security and not disclose passwords to other staff or pupils provided to me by the school or other related authorities.

DATA PROTECTION: I will not give out personal details e.g. mobile phone number/personal e-mail address to pupils. I will ensure personal data is kept secure and used appropriately, whether in school, taken off school premises or accessed remotely. USB pens and other such storage devices will not be used. Staff will make use of 'My School', Office 365 and email to transfer work which can be assessed safely at home without the need for an external storage device. Images of pupils/staff will only be taken, stored and used for professional purposes in line with the school Mobile Devices Policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.
I understand and give permission for my photograph to be displayed in school, used in the school newsletter, school website or for media publications.

C2K INSTALLATION: I will not install any hardware or software on the C2K system without the permission of Mrs McWilliams, (ICT and e Safety Co-ordinator).

USE OF INTERNET AND DEVICES: I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on the C2K system or

iPads. I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Mrs McWilliams or Mrs M McCann, (C2k managers). I will respect copyright and intellectual property rights. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

SOCIAL MEDIA: I understand that any form of Social Media is blocked in school. In my private life, I will take great care to ensure posts are appropriate and make no reference, either directly or indirectly to the school/staff/pupils or events. I will not befriend pupils of the school.

MOBILE PHONES: Due to restricted movement between zones, teaching staff will be permitted to use their mobile phone for communication purposes solely for school business during the school day. All other staff will have their phone on silent and not in use during pupil contact time. Mobile phones will not be used to take photographs/videos of pupils.

PHOTOGRAPHS: I am aware that photos of pupils should not be stored in a portable device such as an iPad, camera or laptop for a prolonged period of time. I will transfer photos regularly to the staff folder or One drive for safe storage and delete from the portable device immediately, in line with Mobile Digital Device Policy. I will adhere to the wishes of parents regarding the publication of pupil photos on the internet or in the media.

I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand it is my duty to report promptly any issues or concerns to the ICT co-ordinator or in her absence, the Principal, using the reporting form.

USER SIGNATURE

I agree to follow this code of safe practice and data protection statement and support the safe and secure use of ICT throughout the school.

Staff Member:_____

Signature: _____

Job Title: _____

Date: _____

Appendix 4

Who can I talk to if I see something **online** I am concerned about?

You can talk to Mrs McWilliams.

She is the ICT and e-Safety co-ordinator.

She is also the Designated Teacher for Child Protection.

You can also talk to:

You class teacher

Any adult in school

Your parents.

Appendix 5

Managing Internet Filtering C2K (C2K Help sheet EN039)

Appendix 6

Reporting a Filtering Concern/Incident

Please fill this form out and give it to Mrs McWilliams, ICT and e-Safety Co-ordinator should you come across a filtering incident which causes you concern. Mrs McWilliams will contact c2k and the necessary steps will be taken to minimise future risk.

Name:	
Date of incident/concern:	
Time of incident/concern:	
Device: Example PC, iPad Provide station number if possible	
Nature and description of image/website or other inappropriate content	
If a website, the URL shown in the browser	
If an image the search term used	
Any other relevant information	
Action taken by ICT and e-Safety co-ordinator (To be filled in by ICT and e-Safety co-ordinator)	