St. Mary's Primary School Cabragh

Online Safety and Acceptable Use of the Internet and Digital Technologies Policy

Date	Policy Reviewed	Policy Amended	Staff Member

Dermot Morrow
UICT Coordinator

Contents

1: Introduction

1.1 Introduction

At St. Mary's Primary we believe that the Internet and other digital technologies are extremely important. With the constantly changing society in which we live it is vital that we provide our pupils with a safe and enjoyable education. The Internet is essential in school, life outside school and for the future. Our school aims to provide resources to encourage our pupils to use the Internet in line with the '5 E's' outlined in the CCEA Curriculum for Using ICT.

The Department of Education in Northern Ireland (DENI) recognises the important role digital technologies have in modern day life stating:
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.
(Circular 2007/1).

The Department of Education makes reference to the Safeguarding Board for Northern Ireland's 2014 report on E-Safety, noting that '*young people's extensive use of technology leaves no doubt over the importance of online safety*' (Circular 2016/27).

With this in mind, we have created a vision statement to reflect this in our school. This policy has been created by the UICT Coordinator in consultation with the Principal to offer guidance on the way forward for safe and sustainable UICT practices in school. It has been approved by the Board of Governors and will be reviewed on a 4 yearly basis and in line with any required changed as implemented by various school-related factors or external agencies.

1.2 Vision

At St. Mary's Primary School we provide an education where all learners feel valued. We strive to educate our pupils to enable them to achieve their potential in all areas of the curriculum. Our mission statement is:

St. Mary's *Primary School promotes a safe, happy, caring and positive environment where all members of our school community are valued, motivated, respected and encouraged to fulfil their potential.*

We teach all elements of Northern Ireland Curriculum (CCEA, 2017) and ultimately aim to equip our pupils for their future lives.

1.3 Rationale for Policy

> *'All schools should have their own E-Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. E-Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills.'*
> DENI E-Safety Guidance (Circular 2013/25)

It is the responsibility of the school, staff, governors and parents to assess the risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related digital technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Online 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 Online 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 communications technologies for educational, personal and recreational use.

1.4 Scope of Policy

This policy applies to all members of the school community who have access to and are users of the school ICT systems, both in and out of the school. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure the online safety of all involved, apply sanctions as appropriate and review procedures.

In relation to online safety incidents that occur outside of school hours, the school will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. Online safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the school community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Incidents of cyber-bullying will be dealt with through the school's Anti-Bullying Policy. Any issues that arise inside school, as a result of online safety incidents outside of the school, will be dealt with in accordance with school policies. This policy works alongside and incorporates other school policies, such as the Safeguarding and Child Protection Policy and the Anti-Bullying Policy.

2: Roles & Responsibilities

2.1 Introduction Statement

At St. Mary's Primary School we understand the importance of online safety and the safe use of digital technologies. The Board of Governors have appointed a number of key staff who are responsible for the implementation of this policy:

Designated Governor for Online Safety:

Principal: Mrs H Lavery

Using ICT Coordinator: Mr D Morrow

Designated Teacher for Safeguarding: Ms L Cush

2.2 UICT Coordinator

The UICT Coordinator (Mr Dermot Morrow) will lead online safety in the school ensuring that the e-Safety policy is implemented in all classrooms. The coordinator has a leading role in creating and reviewing school policies and documents relating to online safety and laisses with technical support staff to ensure that the digital technologies are kept up-to-date:

The UICT Coordinator will:

- Liaise with C2K and other support staff.
- Liaise with the EA and DENI on online safety developments as appropriate.
- Attend cluster meetings with other local primary schools.
- Discuss current issues with the Principal
- Consult with parents and outside agencies as appropriate in relation to online safety education. (REIM)
- Monitor and report to Senior Staff any risks to staff of which the co-ordinator is aware.
- Provide training and advice for staff as appropriate. (Just2Easy and SpellingBlast)
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Monitor the curricular opportunities for implementation of online safety as part of the ICT curriculum.
- Meet with the Designated Teacher for Child Protection (Miss L Cush) to investigate abuse of social network sites by pupils and any other issues in regard to the safe use of the Internet and digital technologies.
- Report to the Board of Governors as required.
- Ensure pupils and staff comply with the Acceptable Use Agreements.

It is a requirement that all staff help to implement these strategies as lead by the UICT Coordinator.

2.3 Designated Teacher for Child Protection

The Designated Teacher for Child Protection (Miss L Cush) will be trained when required in online safety issues as appropriate 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

2.4 The Principal & Board of Governors

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community though the day-to-day responsibility for online safety will be delegated to the designated members of staff. The Principal is responsible for appointing members of staff to act as C2K Managers, and for authorising a Register of Access to the school's confidential files and programmes.

The Principal and UICT Coordinator will be kept informed about online safety incidents.

The Principal will deal with any serious online safety allegations being made against a member of staff.

The Principal is responsible for ensuring that the UICT Coordinator and other relevant staff receive suitable training and allocated time to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Board of Governors is responsible for the approval of the Online Safety and Acceptable Use of the Internet and Digital Technologies Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports from the Principal. Recognising the importance of online safety and given the fact that many of the issues which may arise will be of a safeguarding or child protection nature, the Board of Governors have decided to appoint the Designated Governor for Safeguarding and Child Protection as the Designated Governor for Online Safety. The Designated Governor for Online Safety will regularly review online safety logs as appropriate.

2.5 All School Staff

In addition to the key members of staff outlined above all staff who work at school must be aware of the risks when using the Internet and the requirements for the safe use of digital technologies in school. Staff should ensure:

- They have an up-to-date awareness of online safety matters and follow the current Online Safety and Acceptable Use of the Internet and Digital Technologies Policy as advised by the UICT Coordinator.
- They have read, understood and signed the school's Staff Code of Practice Acceptable Use Policy.
- They report any suspected misuse or problem to the UICT Coordinator or Designated Teacher for Child Protection.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- That students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright laws.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- Undertake all online safety training as organised by the school.
- Pupils understand the Pupil Code of Practice Acceptable Use Agreement.

3: Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.
DENI E-Safety Guidance (Circular 2013/25)

The main areas of risk for the school can be categorised as the content, contract, commercial and conduct of activity.

3.1 Content Risks

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.
Children need to 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.

3.2 Contact Risks

Children may come into contact with someone on-line who may wish to harm them. Some adults use chat rooms online gaming, social media or e-mail to communicate with children for inappropriate reasons.

Children need to be taught:

- That people are not always who they say they are.
- That technology such as voice changing software is available on-line.
- That 'Stranger Danger' applies to the people they encounter through the Internet.
- That they should never give out personal details.
- That they should never meet anyone contacted via the Internet without a responsible adult.

3.3 Commercial Risks

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children need to 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.
- Not to believe everything they see online to be true.

- Be aware of scam emails, how to filter these and be wary of links within these.

3.4 Conduct Risks

Children need to appreciate that bullying, entrapment and blackmail can take place online as well as in person. When connecting with peers and others online, pupils may be in a position where they receive harmful or hurtful statements or threats. Pupils themselves may be involved in issuing such comments or threats.

Children need to be taught:

- To report any such instances to a teacher within school, or to an appropriate adult.
- To seek assistance or help if they feel they are victims of bullying, entrapment or blackmail.
- To understand that their online behaviour is equally as important as that in their real lives and consequences exist for their actions online in their everyday lives.
- Not to send inappropriate images of themselves or others.
- Understand that once published, materials leave a digital footprint online, and will always be traceable or accessible.

If children use the internet in places other than at school, they need to be educated about how to behave online and to discuss problems. They need to be educated as to how to report issues online, such as the instant reporting system provided by CEOP. As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. There are no totally effective solutions to the problems of internet safety. Teachers, pupils and parents must be vigilant.

Many of these risks reflect situations in the offline world and it is essential that this Online Safety and Acceptable Use of the Internet and Digital Technologies Policy is used in conjunction with other school policies, including Positive Behaviour, Child Protection and Safeguarding and Anti- Bullying.

4: Code of Safe Practice

When using the internet, e-mail systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Safe Practice (Acceptable Use Policies) 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 covers fixed and mobile Internet; school PCs, iPads, laptops and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, private iPads, Apple Watches, private laptops and tablets) are subject to the same requirements as technology provided by the

school.

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

4.1 Code of Practice (Acceptable Use Policy) 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.

For pupils in Key Stages 1 and 2, both parties sign the Code of Practice Acceptable Use Agreements and copies of these are held on file by the ICT Co-ordinator. Pupils in Foundation Stage are closely monitored during their use of ICT equipment and are taught to care for equipment and what to do if they see or hear something that upsets them. In addition, the following key measures have been adopted by St. Mary's Primary School to ensure our pupils do not access any inappropriate material:

- The school's Code of Practice for use of the Internet and other digital technologies is made explicit to all pupils and is displayed prominently in suitable locations, such as the ICT suite.
- Our Code of Practice is reviewed each school year and signed by pupils/parents.
- Pupils using the Internet will normally be working in highly-visible areas of the school.
- All online activity is for appropriate educational purposes and is supervised, where possible.
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group.
- Where the task involves pupils locating suitable websites themselves, explicit instruction will be provided by teachers of how best to locate appropriate sites, and how to evaluate their authenticity and appropriateness.
- Pupils in all Key Stages are educated in the safe and effective use of the Internet, through a number of selected programmes.
- It should be accepted that however rigorous these measures may be, they can never be 100% effective. Neither the school, nor C2K or Call Tech Support, can accept liability under such circumstances.

4.2 Code of Practice (Acceptable Use Policy) for Staff

Staff are aware of the important role they play in promoting and protecting pupils' safe use of digital technologies. Each year members of staff using the school's ICT systems sign and agree to the Acceptable Use Agreement for Staff. Staff have also agreed that:

- Pupils accessing the Internet should be supervised by an adult at all times.

- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in prominent locations within the school and discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- Recommended websites for each year group have been approved by class teachers. Any additional websites used by pupils should be checked beforehand by teachers to ensure, as far as possible, 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 UICT Co-ordinator.
- In the interests of system security, staff passwords should not be shared.
- Teachers are aware that the C2K My School system tracks all internet use and records the sites visited. The system also logs emails and messages sent and received by individual users. It is important that users are aware that a request may be made by the Principal to access such tracking information, and by signing the Acceptable Use Policy for Staff, members of staff authorise such information to be released to the Principal/Boards of Governors.
- 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.
- Staff understand that any work carried out on the C2k system whilst in the employment of St. Mary's Primary School remains the property of the school.
- Photographs of pupils should, where possible, be taken with a school camera or iPad and images stored on a centralised area on the school network, accessible only to staff (Staff Drive)
- School systems may not be used for unauthorised commercial transactions.

4.3 Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's discipline policy. Minor incidents will be dealt with by the UICT Co-ordinator and in consultation with the Principal, and may result in a temporary or permanent ban on Internet use.

In the first instance, for minor breaches of the Acceptable Use Policy by pupils, a reminder of the AUP will be given. On a second breach, and for more serious incidents as identified by the UICT Co-ordinator, the incident will be recorded in detail within the school's Online Safety and Acceptable Use Incident Log. Incidents involving child protection issues will be dealt with in accordance with school safeguarding and child protection procedures. Where incidents of technology misuse involve members of staff, and it is deemed warranted by the Principal, they will be dealt with by the Board of Governors through the normal disciplinary measures. Within all circumstances, where a potential breach of online safety has occurred, it will be registered in the school's Securus Incident Log or Online Safety and Acceptable Use Incident Log.

5: Online Safety

In St. Mary's Primary School we believe that, alongside having a written safety policy and acceptable use agreements, 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 as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

5.1 Internet Safety Awareness for Pupils

Rules for the acceptable use of the Internet are discussed with all pupils and are prominently displayed in key areas in the school. In addition, online safety is incorporated into planning for UICT across the curriculum, including Internet Safety Awareness using a range of online resources. E.g. taking part in Internet Safety Day and other appropriate events throughout the year. The Online Safety Curriculum is delivered to all pupils from Primary 1 to Primary 7.

5.2 Internet Safety Awareness for Staff

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and attends regular courses and cluster meetings as appropriate. This training is then disseminated to all teaching staff, classroom assistants and support staff on a regular basis.

Points for Teachers to Consider:

- Internet and digital technology use should be planned, task orientated and educational within a regulated and managed environment. Supervision is the key strategy. Children should have a teacher or classroom assistant present when using the internet (this is essential with iPad use). Computers and iPads should be positioned, as far as possible, so that itis possible for adults to see materials on screen. allowing the teacher to monitor and freeze screens of individual pupils. iPads use should not be encouraged during break and lunch times when the class teacher is not present, and no structured task has been set.
- Children should know why they are using the internet and digital technology. We should teach children to use the internet in response to a need, e.g. to answer a question which has arisen from work in class.
- Search engines require careful use and planning/supervision. Children can be bombarded with information and yet fail to find the material they need.
- Children do not need thousands of website addresses. A small appropriate choice is much more effective.
- Pupils need explicit instruction in how best to locate and evaluate websites.

- Pupils should not use private email servers on school property. Such activity is filtered through the C2K software.
- Discuss with pupils the rules for responsible internet use. It is not enough to protect children from materials, we must teach them to become online safety wise. Children need to learn to recognise and avoid the risks. Children need to know what to do if they come across inappropriate material or if they are approached by a stranger. This links with our Online Safety Curriculum.

5.3 Internet Safety Awareness for Parents

The Acceptable Use Policy and Online Safety Policy are available for parents by request. The Acceptable Use Policy for pupils is sent home at the start of each pupils first day of school for parental signature.

Points for Parents to Consider:

It is important to promote Internet Safety in the home and to monitor Internet use. Keep the computer in a communal area of the home.

- Ask children how the computer works.
- Monitor online time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing.
- Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information on the Internet.
- 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 on-line.
- Be aware that children may be using the internet in places other than in their own home or at school.
- Be aware of the vast array of apps available to pupils on their mobile phones and other mobile technical devices, with particular attention to the minimum age for use of such software.
- Check parental control settings on devices which connect to the internet.
- Consider keeping your WIFI password private from children, so they cannot share it with their friends when they visit your house. Remember that any activity which visitors to your home undertake whilst using your internet access point is traceable to your address and thus may be deemed your responsibility.

5.4 Community Use of School ICT Resources

The school's ICT facilities may be used as a community resource under the Extended Schools programme. This could be in the form of both school and outside agency led courses. Users are issued with separate usernames and passwords by C2K. They must also agree to the school's Code of Practice Acceptable Use Policy before participating and only access pre-selected and appropriate websites under the guidance of an approved person as designated by the Principal/Board of Governors.

5.5 Teaching and Support Staff: Password Security

Password security is essential for staff, particularly as they are able to access and use student data.

- Staff are expected to have secure passwords which are not shared with anyone or written down in a visible location.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.
- Staff should ensure iPads are secured appropriately and also ensure that they are kept secure if removed from the school.

5.6 Students: Password Security

- All users read and sign a Code of Practice Acceptable Use Agreement to demonstrate that they have understood the school's Acceptable Use Policy.
- Students are expected to keep their passwords secret and not to share with others, particularly their friends. In upper Key Stage 2 pupils should be encouraged to select an appropriate secure password of their own.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Pupils should be made aware of dangers using their C2K password at home to access C2K resources, particularly on a shared device.

5.7 Health and Safety

St. Mary's Primary School has attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards, Digital Projectors, computers, laptops and iPads are being used.

5.8 Digital and Video Images of Pupils

Parental permission is sought at the start of each school year to cover the use of photographs of pupils on the school website, in the local press and for displays etc within school and written permission must be obtained from the parent/carer. This information is held securely by the office staff and can be requested by teaching staff as required.

5.9 School Website

Our school website (www.stmaryscabragh.com) promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life through individual class pages and news stories. 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, however individual images and names can be used to celebrate individual successes all with parental permission
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.
- Website links selected by teachers may be put on the website for pupils to access outside of school – sites will be previewed and checked regularly.
- Parents'/Carers' permission will be sought to publish pupils work and/or photographs. These will only be published subject to the safeguards above.
- Access levels will be put in place for the website:
    1. Admin User – Mrs L Quinn(Principal)
    2. Contributor – All other teaching staff

5.10 Storage of Images

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network, accessible only to teaching staff (Staff Drive).

5.11 Mobile Phones

Pupils have no need to use mobile telephones whilst in school. Should emergency contact between parents and pupils be required, then the school office staff are available to relay such emergency information. The school accepts no liability for devices brought into school. Mobile phones are not permitted to be used by pupils on school grounds or on school trips. They should be handed to Mrs L Quinn or Mrs P O'Neil in the school office who will keep them locked away safely until the end of the school day. If a pupil breaches the school policy, then the phone or device will be confiscated

and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or guardians by the Principal.

5.12 Social Networking Platforms

Chatrooms, blogs and other social networking sites are blocked by the C2K filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our internet safety education for pupils.

Instances of cyber-bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's Discipline Policy and child protection procedures. Both parents and pupils should be aware that messages relating to individual members of staff or the school which are derogatory in nature may be reported to the Police Service of Northern Ireland, who may treat such instances as harassment.

The school maintains a Facebook page, recognising the value of social networking sites for communicating more effectively with parents in the 21st century. Access to these pages is strictly controlled and available only to the UICT Coordinator and Principal.

6: GDPR, The Data Protection Act & Filtering

6.1 The EU General Data Protection Regulation & The Data Protection Act

The school complies with the EU GDPR and the Data Protection Act, and staff are regularly reminded of their responsibilities. The Principal is responsible for authorising a Register of Access to the school's data. 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 or locked 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, the following guidance must be followed:

- The device is password protected with appropriate encryption software.
- 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.

The school has in place a comprehensive Data Protection Policy and Privacy Notices, which are available from the Principal and school office on request.

6.2 Breaches of Filtering Systems

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

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the internet and digital technology may give children access to undesirable information or images.

Children are regularly reminded that should they encounter inappropriate material on-line they must immediately leave the website and inform an adult.

Should a child or teacher encounter unsuitable material through the managed service, this should be reported immediately to the ICT Co-ordinator and this will then be reported to C2k.

7: Policy Review

7.1 Statement for Policy Review

This policy will be reviewed annually by the Using ICT Coordinator due to the constantly changing world of ICT and technology in society.

All staff will be made aware of any relevant changes.

BRING YOUR OWN DEVICE (BYOD) USER AGREEMENT - STAFF DECLARATION

I request permission to use my own personal ICT device(s) in school.

Device 1:	
Device 2:	
Device 3:	

I have read and understood the Online Safety and Acceptable Use of Internet and Digital Technologies Policy and I agree to be bound by all guidelines, rules and regulations contained within it. I agree to use the device for educational use only.

Disclaimer - please read carefully

The school accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school activities. The decision to bring a personal ICT device into school rests solely with the member of staff, as does the liability for any loss/damage.

I understand the disclaimer and accept that I am personally and solely responsible for the correct care, safety and security of the device. I understand that the school accepts no liability in respect of any personal ICT device used in school by a member of staff.

I understand that I may only connect to the school's filtered Wi-Fi networks, with the permission of the principal or UICT Coordinator and for school business only, once I have signed and returned this BYOD agreement, and agree that I shall not try to circumnavigate or diminish the filtering security of the networks.

I am aware that the C2K My School system tracks all internet use and records the sites visited. The systems also log emails and messages sent and received by individual users and log all activity. It is important that users are aware that a request may be made by the Board of Governors, through the Principal, to access such tracking information, and by signing the Acceptable Use Agreement for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.

This contract will remain in force throughout my time at school and it may be revised to take account of technological advancements in the interests of pupil and staff safety. Should I change my device, I agree to update this record with the UICT Coordinator.

Please complete and return this form to the UICT Coordinator.

PRINT Name:		**Date:**	
Signature:			

Code of Practice
Acceptable Use of the Internet and Digital Technology: Pupils

Pupil's Name: _____ Class: _____

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 also realise that this agreement extends to the use of any technology or device on school premises, whether personally or school owned.

Please discuss these guidelines with your child and stress the importance of the safe use of digital technology, including the Internet and agree that, as a pupil at St. Mary's Primary School:

- I will take very good care of all equipment I use in school, treating it with respect.
- On the C2k network and any other appropriate apps, I will only use my own login username and password.
- I will keep my username and password private and report any log in problems to my teacher.
- 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 accessing any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only both in the ICT Suite or on an iPad.
- I understand that I am not allowed to access any private email accounts I may have whilst in school.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed.
- I understand that I am not allowed to enter internet chat rooms while in school.
- If I see anything, I am unhappy with or I receive messages I do not like, I will tell a teacher.
- I will not bring in memory sticks or hard drives 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 I must not bring a mobile phone to school.
- I understand that I am not allowed to bring my own personal devices to school without the prior permission of the Principal/ICT Co-ordinator and that I must not try to connect any device to the school's networks.
- I understand that if I deliberately break these rules, I could be stopped from using the internet/digital technologies, my Parent/Guardian will be informed and sanctions will apply.
- I understand that the school computer/iPad systems log and monitor my use of the devices.

Parents/Guardians

As noted in the school's Online Safety and Acceptable Use Policy, both parents and staff have an important role to play in educating children on how best to use digital technology safely. As parents, it is important to seek to monitor and protect your child's online activity at home. We all, parents and teachers should remember that we are important role models in the lives of our children. We must all remember that any digital communication, such as social networks, are still subject to the rule of law. We must work together in partnership to educate our children and keep them safe online.

Pupil Signature:		**Parent Signature:**	
Date:		**Date:**	

Code of Practice Acceptable Use Agreement: Staff

The computer system and associated digital technology, including staff and pupil iPads, 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 Acceptable Use Policy has been drawn up to protect all parties – the students, the staff and the school.

By signing this agreement, you recognise and accept that the Board of Governors reserves the right to examine or delete any files that may be held on its computer system, to monitor any Internet sites visited and to monitor and review the use of the school's digital technology.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the UICT Coordinator. By signing, members of staff accept and agree that:

- All Internet activity and use of digital technology should be appropriate to staff professional activity or the pupils' education.
- Access should only be made using authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school's 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.
- 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 and could be reported to the Police.
- When using school's social media accounts all posts and activity must be appropriate and acceptable, reflecting the ethos and values of the school.
- 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.
- Staff understand that any work carried out on the C2k system whilst in the employment of St. Mary's Primary School remains the property of the school.
- Photographs of pupils should, where possible, be taken with a school camera or school iPad and images stored on a centralised area on the school network, accessible only to staff. In the 'Staff' Folder.
- School systems may not be used for unauthorised commercial transactions.
- Members of staff agree to maintain the confidentiality of records and information held digitally within the school, insuring they meet the requirements of the GDPR and the Data Protection Act.
- Staff should not be directly connected on social media to pupils at the school. They should also ensure that their social media does not give cause for the school to be called into disrepute.
- Staff should not use mobile phones in the presence of children within classrooms. During the teaching day, mobile phones should remain out of sight from children, unless authorised by the Principal. Staff should, as far as possible, seek to use their mobile phones in the staffroom or office away from pupils.
- Staff accept that they may not connect personal devices to the school's networks, including the C2k Wi-Fi networks, without accepting and returning to the UICT Coordinator a form of agreement to the school's Bring Your Own Device Policy and after consultation with the Principal or UICT Coordinator.

Teachers are aware that the C2K My School tracks all internet use and records the sites visited. The systems also log emails and messages sent and received by individual users and log all activity. It is important that users are aware that a request may be made by the Board of Governors, through the Principal, to access such tracking information, and by signing the Acceptable Use Agreement for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.

Name:	
Signed:	
Date:	