St. Mary's Newtownbutler

E-Safety Policy

Including

Acceptable Use Agreement

and Implementing E-safety.

Introduction

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

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- 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 we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach 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. '360 Degrees Safe', the e-safety self-review tool, has been used by staff, in formulating this policy.

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. 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 are:

Potential Contact

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

Children should be taught:

- That people are not always who they say they are.
- That people they encounter through the Internet may be dangerous.
- That they should never give out personal details or
- That they should never meet, alone, anyone contacted via the Internet, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

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.

Children should be taught:-

- That information on the Internet is *not always* accurate or true.
- To question the source of information.
- How to respond (or not!) to unsuitable materials or requests and to tell a teacher/adult immediately.
- Not to pass indecent images to any third party and that doing so is breaking the law.

Excessive Commercialism

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

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 on-line and to discuss problems. There are no *totally effective* solutions to problems of Internet Safety. Teachers, pupils and parents must be vigilant.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-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 expected to incorporate e-Safety activities and awareness into their lessons, when appropriate.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers 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 website contains useful information and links to sites like CEOP's "thinkuknow" website, Childline, and the CBBC Web Stay Safe page.

- The school will communicate relevant e-Safety information through newsletters and the school website.

Parents should remember that it is important to promote e-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 on-line 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 and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- St Mary's will plan and provide opportunities within a range of curriculum areas to teach e-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 e-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/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- 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 Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.
- Children are taught about digital footprints

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail or other form of message.
- 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 e-mail addresses. In some instances, children may have access to a group e-mail 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 will 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.
- Our pupils are asked to report any incidents of bullying to the school.
- 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.
- Pupils are not allowed to use personal mobile devices/phones (in school) during class.
- Staff should not use personal mobile phones during designated teaching sessions.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. 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/carers 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 will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

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 e-Safety rules. These e-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 e-Safety rules and within the constraints detailed in the school's e-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, MIS systems.

Handling e-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 Co-ordinator and recorded in the e-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.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. 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/ Internet Safety Day.

- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance 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.

Roles and Responsibilities

As e-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. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The ICT / E-Safety Co-ordinator liaises regularly with the Safeguarding Team and meets annually with the Designated Governor for Child Protection. Mrs Clare Leonard is Designated teacher for Child Protection, Mrs Kelly and Miss Therez McGuigan are deputy designated teachers for Child Protection. All governors are regularly updated on the issues at our school in relation to local and national guidelines and advice. Mr Eoghan Casey has been designated as governor responsible for Child Protection.

Monitoring and review:

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

This policy is the Governors' responsibility and they will review its effectiveness bi-annually. They will do this during reviews conducted between the ICT Co-ordinator and the Designated Child Protection Team.

Writing and Reviewing the e-Safety Policy

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 is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

Implementing E-safety

Pupils

The education of pupils in e-safety is essential. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience. The aim is to develop children's e-safety skills for when they are in school and outside of school.

E-Safety education should be provided in the following ways:

- Planned e-safety activities should be incorporated into PDMU and other lessons, where appropriate. (For e.g. within literacy – creating a poster/news sheet, reading non-fiction texts, giving a presentation etc.)

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and whole school activities e.g. participation in an Internet Safety Week or Safer Internet Day. Visit from PSNI.

- Children should research e-safety and become familiar with key websites such as www.thinkuknow.co.uk and use the information to create resources to raise parental/peer awareness of safety messages. The children can create posters, presentations, short films or podcasts on e-safety and display these within school and at home. (e-safety can be the focus for many CCEA tasks)

- Encourage children to discuss e-safety with parents/carers – look at a website together, discuss an e-safety poster etc. This can form part of a homework task.

- SMART safety rules should be displayed in classrooms and should be discussed and referred to regularly.

- Children should participate in devising and agreeing to an AUP and encouraged to adopt a safe and responsible use of ICT, the internet and mobile devices both within and outside school.

- The School Council or After School ICT Club may focus on e-safety issues.

Parents / Carers

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's online experiences. Parents often either underestimate, or do not realise, how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school should therefore seek to provide information and awareness to parents and carers in the following ways:

- Put links to e-safety information and resources on the school website.
- Include e-safety tips on the school website – embed the *"Childnet" banner.
- Use opportunities when parents/carers are in school - provide leaflets at parent interviews, curriculum evenings, open days, parent assemblies, etc.
- Have children carry out e-safety research with parents and discuss web materials, posters etc.
- Put e-safety tips in the school newsletter.
- Share the e-safety policy – make it available on the school website and in the school.
- Display e-safety information where parents/carers gather in the school at collection points. www.childnet-int.org/publications/resources.aspx

Staff

Staff should be involved in formal discussions about e-safety and have opportunities to participate in e-safety training. An audit of the e-safety training needs of all staff may be carried out.

- The ICT Coordinator will keep up to date on e-safety through attendance at INSET and by reviewing guidance documents released by agencies such as CEOP/DE/EA and others. The ICT Co-ordinator should seek planned opportunities to disseminate this information to all staff.

- The E-Safety Policy should be discussed and reviewed by staff during staff meetings or on INSET days.

- Staff should be familiar with e-safety websites such as Childnet's "Know it all for Teachers" or CEOP's "ThinkuKnow". (see below)

- Implementing E-safety may be part of agreed PRSD targets for the whole school.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies.

- Teachers should share good practice in implementing e-safety and ensure e-safety activities are included in planning for PDMU and other curriculum areas.

Governors

Governors should be encouraged to take part in e-safety training or awareness sessions. This has particular importance for those who are members of any sub- group involved in health and safety /child protection.

This may include:

- Attendance at e-safety events.

- Participation in school training/information sessions for staff or parents.

- The ICT Co-ordinator meeting with the Governors to update them on e-safety issues and procedures within the school.

- Consultation with regard to the e-safety Policy.

- Accessing e-safety information which is available on the school website or in parent leaflets and newsletters.

This e-Safety policy and its implementation will be reviewed bi-annually.

Approved by the Board of Governors **Date: April 22**

_____

Rev Fr M King (Chair of Board of Governors)

Planned Review : April 2024

Appendix 1: Social Media Policy

Social Media Policy

Rationale
This policy is to safeguard and minimise the reputation of the school, staff and the wider community through the use of social media. It applies to the use of social media for work and personal purposes, on equipment used by staff inside school or at home (including non-school appliances). The policy wishes to make sure staff are not making themselves vulnerable.

Scope of Policy
This policy covers all staff, pupils, governors, volunteers, placement students. They will be collectively referred to as *Staff* in this policy. Parents or community users who have access to our equipment are also required to comply with this policy.

This policy deals with the use of all forms of social media, including Facebook, YouTube and Twitter, and all other social networking sites, internet postings and blogs. It applies to use of social media for school purposes as well as personal use that may affect the school in any way.

1. **School Use of Social Media**

Staff setting up a school account should:

- **Notify the Internet Safety Co-ordinator, Mrs Grew, and forward details (intended audience, platform, staff in charge and shadow member of staff). This should be recorded by Mrs Grew and Mrs Kelly should be informed.**
- **Staff should regularly monitor, update and manage the content posted.**
- **Staff should ensure all pupils understand and agree with the guidelines.**
- **Staff should report any online incidents to Mrs Grew**
- **Ensure communication is professional**

2. **Personal/ Private Use of Social Media**

Staff are permitted to use social media for personal purposes, outside of school working hours.

3. Guidelines for Responsible Use
3.1 Staff must not post disparaging or defamatory statements about:

1. **The school**
2. **Current, past or prospective Staff (as defined in this policy)**
3. **Current, past or prospective pupils or their parents/carers/families**
4. **The school's suppliers and service providers; and**
5. **Other affiliates or stakeholders**

3.2 Staff should avoid social media communications that might be misconstrued in a way that could damage the school's reputation, even indirectly. Staff should be respectful when making any statements.

3.3. Ensure profile and any content posted are consistent with the professional image you wish to present.

3.4 If you disclose your affiliation with the school on your profile or in any social media postings, you must state that your views do not represent those of your employer.

3.5 Staff should not accept as a 'friend' any pupil currently enrolled at the school or any past pupil under the age of 18. The exception to this is if the pupil is a family member. Staff should exercise their own discretion in this case.

3.6 Staff should ensure that their settings on social media are set in such a way that protects their privacy. This applies to all postings, photographs and images.

4. Social Media: Prohibited Use

a. **Avoid communications that could damage the school's reputation, even indirectly.**
b. **Do not use social media to defame or disparage the school, management, staff, or any third party**
c. **Do not use social media to harass, bully or unlawfully discriminate against staff or third parties**
d. **Do not use social media to make false or misleading statements**
e. **Do not use social media to impersonate colleagues or third parties**
f. **Do not express opinions on the school's behalf, unless expressly authorised to do so**
g. **Do not include the school logo in any posting or in your profile**
h. **Do not post comments about pupil performance**

Any misuse of social media should be reported to Mrs Grew (Internet Safety Co-ordinator) or Mrs Kelly.

Appendix 2

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- **that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.**
- **that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.**
- **that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.**

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: .....
Pupil Name: .....

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

- ***I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.***

- ***I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.***

- ***I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.***

- ***I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.***

Signed: .....
Date: .....

Appendix 3

Acceptable Use Policy Agreement -KS2

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 systems and other users.

For my own personal safety:

- **I understand that the school will monitor my use of the systems, devices and digital communications.**
- **I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.**
- **I will be aware of dangers, when I am communicating on-line.**
- **I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)**
- **I will seek my parent's permission before meeting anyone I have met online.**
- **I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.**
- **I understand that the school *ICT* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.**

I will act as I expect others to act toward me:

- **I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.**
- **I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.**
- **I will not take or distribute images of anyone without their permission.**

I understand that I am responsible for my actions, both in and out of school:

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form-KS2

This form relates to the pupil Acceptable Use Agreement; to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- **I use the school ICT systems and devices**
- **I use my own equipment out of the school in a way that is related to me being a member of this school e.g., communicating with other members of the school, accessing school email, MY SCHOOL, website etc.**

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Appendix 4

Pupil Acceptable Use Policy Agreement for Foundation pupils

This agreement has been discussed in school with your child. Please reinforce these messages at home, sign below on behalf of your child and return to the class teacher.

This is how we stay safe when we use computers:

- **I will ask a teacher or suitable adult if I want to use the computers / tablets**
- **I will only use activities that a teacher or suitable adult has told or allowed me to use**
- **I will take care of the computer and other equipment**
- **I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong**
- **I will tell a teacher or suitable adult if I see something that upsets me on the screen**
- **I know that if I break the rules I might not be allowed to use a computer / tablet**

Signed (parent): .....

Appendix 5

Pupil Acceptable Use Policy Agreement for KS1 pupils

This is how we stay safe when we use computers:

- **I will ask a teacher or suitable adult if I want to use the computers / tablets**
- **I will only use activities that a teacher or suitable adult has told or allowed me to use**
- **I will take care of the computer and other equipment**
- **I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong**
- **I will tell a teacher or suitable adult if I see something that upsets me on the screen**
- **I know that if I break the rules I might not be allowed to use a computer / tablet**

Signed (child): .....

Appendix 6

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on Seesaw, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent / carer permission for taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their full names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

Digital / Video Images Permission Form

Parent / Carers Name: ..... **Student / Pupil Name:** .....

As the parent / carer of the above pupil, I agree to the school taking digital / video images of my child / children.	**Yes / No**
I agree to these images being used:	
• **to support learning activities.**	**Yes / No**
• **in publicity that reasonably celebrates success and promotes the work of the school.**	**Yes / No**
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	**Yes / No**

Signed: .....

Date: .....

Appendix 7

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy
New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- **that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.**
- **that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.**
- **that staff are protected from potential risk in their use of technology in their everyday work.**

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- **I understand that the school will monitor my use of the school digital technology and communications systems.**
- **I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, MY SCHOOL etc.) out of school, and to the transfer of personal data (digital or paper based) out of school**
- **I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.**
- **I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.**

- **I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.**

I will be professional in my communications and actions when using *school* ICT systems:

- **I will not access, copy, remove or otherwise alter any other user's files, without their express permission.**
- **I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.**
- **I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / MY SCHOOL) it will not be possible to identify by name, or other personal information, those who are featured.**
- **I will only use social networking sites in school in accordance with the school's policies.**
- **I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.**
- **I will not engage in any on-line activity that may compromise my professional responsibilities.**

The school and the EANI have a responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- **When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. Any USB device I use for school related information will be encrypted / password protected.**
- **I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)**
- **I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.**

- **I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.**
- **I will not disable or cause any damage to school equipment, or the equipment belonging to others.**
- **I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.**
- **I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.**
- **I will immediately report any damage or faults involving equipment or software, however this may have happened.**

When using the internet in my professional capacity or for school sanctioned personal use:

- **I will ensure that I have permission to use the original work of others in my own work**
- **Where work is protected by copyright, I will not download or distribute copies (including music and videos).**

I understand that I am responsible for my actions in and out of the *school*:

- **I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.**
- **I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.**

Staff (and Volunteer) Acceptable Use Policy Agreement

This form relates to the Staff (and Volunteer) Acceptable Use Agreement, which is attached.

I confirm that you have read and understood the agreement and will use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Staff should retain the agreement and return this signed page to Mrs Grew (E-Safety Co-ordinator).

Appendix 8

Internet Access: Additional Advice for Parents

1. **A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.**

2. **Parents should agree with their children suitable days/times for accessing the Internet.**
3. **Parents should discuss with their children the rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use.**
4. **Parents should get to know the sites their children visit and talk to them about what they are learning.**
5. **Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below).**
6. **It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.**
7. **Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.**
8. **Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school, they should immediately inform the school.**

Further advice for parents is available from the following sources:

- **http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.**

- **http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.**

- **http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.**

- **http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.**

- **http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.**

- **http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)**

- **http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use**

Appendix 9

Use of Mobile Phones and other Electronic Devices
Rationale

The Board of Governors of St. Mary's Primary School wish to ensure that all pupils are safe and well cared for. All staff and pupils have a right to work, enjoy and learn in a secure and caring environment. They also have a responsibility to contribute to the protection and maintenance of such an environment. The use of increasingly sophisticated equipment and integrated cameras could present a number of problems, hence, the co-operation of parents and carers with this guidance is very much appreciated.
It is therefore school policy to prohibit the unauthorised use by pupils of mobile phones or other electronic devices while on our school premises, grounds or on trips or activities e.g. school swimming.

In an emergency situation, and with the express approval of a senior member of the school staff, or where a written request has been received from the parent/carer, the device may be stored in the school office. It is the child's responsibility to ask for the device at the end of the school day. Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office (02867738690).

The school accepts no liability for the loss or damage of any electronic device which is in the pupil's possession during the school day.

If a pupil is found by a member of staff to be using a mobile phone/electronic equipment for any purpose, the device will be confiscated from the pupil. The pupil must arrange for their parents/guardians to collect confiscated equipment from the School Office during normal working hours.

Inappropriate photographs or video footage with a mobile phone or other electronic device of other pupils or teachers will be regarded as a serious offence and disciplinary action will be taken.

This policy supports the school's Health and Safety and Safe Guarding Policies: Anti-bullying, Child Protection, Positive Behaviour and Internet Acceptable Use policies. It has been endorsed by the Board of Governors and will be monitored, reviewed and amended as required.

Approved by the Board of Governors
Reviewed

Appendix 10

Help Advice and Information

E-Safety - Useful Websites

For Children
www.thinkuknow.co.uk includes sections for teachers, parents, children
www.bbc.co.uk/cbbc/help/web/staysafe
www.kidsmart.org.uk – includes sections for teachers, parents, children

For Teachers
www.childnet-int.org/kia/primary/
www.learn-ict.org.uk/primary.asp
www.childnet-int.org/publications/resources.aspx
https://swgfl.org.uk/services/project-evolve/

For Parents/Carers
www.childnet-int.org/kia/parents/
www.google.co.uk/goodtoknow/online-safety
www.kidsmart.org.uk/parents
www.bbc.co.uk/webwise/
www.bbc.co.uk/cbeebies/grownups/help/social-media
www.bbc.co.uk/onlinesafety/

Keep Our iPads

Stay away from liquids

Always use two hands

Follow instructions

Enjoy this technology
& treat it with respect!

This is how I stay safe when I use the iPad:

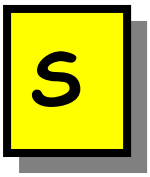
- ✓ I will protect the iPad and carry it carefully in its case
- ✓ I will keep food and drinks away from the iPad as they may damage it
- ✓ I will not change the settings on the iPad without adult permission
- ✓ I will only use activities on the iPad that a teacher/classroom assistant had allowed me to use
- ✓ I will tell a teacher or classroom assistant if I see something that upsets me on the screen
- ✓ I will use the camera when the teacher tells me and photograph people with permission
- ✓ I will never share images or movies on the internet, unless I am instructed to by my teacher
- ✓ I will abide by the school's Internet Safety rules

I know that if I break the rules, I might not be allowed to use the iPad for some time.

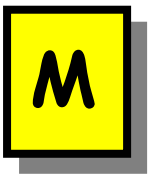

Childnet International
www.childnet.com
Be smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
M
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
A
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
R
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
T
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Safety Rules For Children

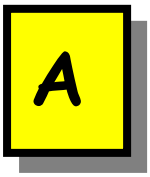
Follow These SMART TIPS



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

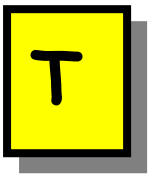


Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees