**E-Safety Policy**

**(Incorporating Acceptable Use Policy)**



**St. Mary’s Primary School**

**Greenlough**

**September 2022**

|  |  |
| --- | --- |
| **DATE** |  |
| **Chair of Board of Governors** |  |
| **Principal** |  |
| **Date of Review** | **September 2025** |

1. Introduction

The Board of Governors will ensure that St. Mary’s Primary school has a policy on the safe, healthy, acceptable and effective use of the Internet and other digital tools e.g. digital cameras. They also promote safe and acceptable practices for all staff and pupils.

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 and Wikis

# Podcasting

# Video Broadcasting

# Music Downloading

# Gaming

# Mobile/Smart phones with text, video and/or web functionality

# Other mobile devices with web functionality

# Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

# The staff and governors of St. Mary’s Primary understand their responsibility to educate our pupils in e-Safety issues. We aim to teach children 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.

# E-Safety is short for electronic safety.

# It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

# **E-Safety in the school context:**

# is concerned with safeguarding children and young people in the digital world;

# emphasises learning to understand and use new technologies in a positive way;

# is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;

# is concerned with supporting pupils to develop safer online behaviours both in and out of school; and

# Is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

# The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The school’s e-Safety policy reflects this by keeping abreast of the changes taking place. Our school has a duty of care to enable pupils to use on-line systems safely.

**2. General**

Use of ICT in the Northern Ireland education community must be in support of the aims and objectives of the Northern Ireland Curriculum

* + - All users must comply with all copyright laws;
    - All users must limit their use of the Internet for school related purposes – examples of this include the use of email, the use of the Internet to investigate and research school subjects and staff using the Internet to further develop their professional development;
    - All users are expected to behave in an appropriate manner when communicating with others;
    - All users must be aware that the use of the Internet in schools is a privilege and not a right and this privilege will be withdrawn if it is misused;
    - All users must respect the hardware and software that has been made available to them;
    - All users must respect the work of others.

**3. Code of Conduct for Staff (See Appendix 1)**

All staff annually read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

**4. Code of Conduct for Pupils (See Appendix 2A)**

Pupils will be taught that the responsible and safe use of the internet 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 Acceptable Use Rules & SMART Tips (KS2) (Appendix 2B).

These e-Safety rules will also be displayed clearly in all rooms.

Teachers will revise these e-safety rules with their class at the start of each term.

* + - I will access the system with my login and password.
    - I will not access other people’s files without permission.
    - I will only use the computers, Internet, My School for school work and homework.
    - I will not bring in software or any USB Hardware into school without permission.
    - I will ask permission from a member of staff before using the Internet.
    - I will only e-mail people I know, or my teacher has approved.
    - I will not open e-mails sent by someone I don’t know and report any unpleasant material or messages sent to me.
    - The messages I send will be polite and responsible.
    - I will not give my name, home address, telephone number, or arrange to meet someone.
    - I will not bring a mobile phone or any device which receives internet, takes photos or videos into school.
    - I understand that the school may check my computer files and may monitor the Internet sites I visit.
    - I will never give out personal information.

**5 Pupil Sanctions (Appendix 5)**

Pupils must follow the St. Mary’s Primary School Acceptable Use Agreement for pupils. Any violation of the regulations (See Appendix 2A) is unethical and may constitute a criminal offence. Should any violation be committed;

1. Access privileges may be revoked; and

2. School disciplinary action in line with the school discipline policy and/or appropriate legal action may be taken.

Use of the school’s Internet account is a privilege, not a right.

The Internet is to be used for educational and research purposes only, consistent with the educational aims of the School. Misuse will result in loss of the account.

Staff may monitor pupil use of the Internet, including e-mail, to determine that use is for the stated purposes. For this and other reasons, e-mail is not private. Violations that may lead to cancellation of Internet access include:

* Playing inappropriate computer based games;
* Downloading excessive large files/inappropriate software/apps;
* E-mail correspondence inappropriate to educational purposes;
* Any activity posing potential risks to themselves or others;
* Harassing other users (e.g. with unwanted e-mail messages);
* Illegal activity;
* Revealing any person’s home address/phone number;
* Vandalism of accounts or systems;
* Using abusive, vulgar, or other inappropriate language;
* Viewing or downloading inappropriate images;
* Failure to report known security problems; and
* Any other inappropriate use or misuse of the facility.

Staff at St. Mary’s Primary School will deem what is inappropriate use, and their decision is final. Accounts are monitored and use of the account implies agreement to such monitoring. Staff may close an account at any time for violations and/or for the safety of the child using the account.

**6 Parental Responsibility (Appendix 2b & 3)**

* Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child and/or with 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. Appendix 3
* Parent should be aware that they may withdraw photographic/video permission at any stage but must do so in writing.

**7 Information for Parents (See Appendix 2b and 3)**

* Parents should, in co-operation with staff, make pupils aware of the rules and expectations within the Code of Conduct Agreement. (Appendix 2b)
* Parents should be aware that the access to the Internet provided to staff and pupils in school has limiting security features.
* Parents should be aware that the use of the Internet in school is closely monitored by staff.
* Parents should be aware that there will be no use of the Internet without the supervision of staff and that this will be in full view of others, e.g. the classroom or ICT Suite.
* Parents should be aware that the use of ICT is used as a tool to complement and enhance prior learning– i.e. the use of computers, iPads etc.
* Parents should be aware of the images they take and where and when they use them. Posting images onto any Social Media Websites or using material without the permission of other parents is illegal and taken seriously by the PSNI. (Appendix 3)
* Parents should be aware that children’s full names will not be available online at any stage but their work may be displayed on the School Website and social media platforms only where permission has been given.
* Parents should be aware that no photographs of pupils will be available online without parents giving their permission. Group and individual photographs will be used excluding the pupils’ full names.
* Parents should be aware that pupils are not permitted to bring mobile phones into school or on school trips, as Internet access becomes very difficult to monitor.
* Parents should also be aware that social networking sites such as Snapchat, Facebook and Twitter adhere to a strict ‘over 13s’ age policy.
* Parents should be aware that the School Website contains useful information and links to sites like thinkuknow, Childline, Safer Internet Day website, BBC Learning Zone, EA.
* Parents should be aware that the school will communicate relevant e-Safety information through newsletters and the school website.

**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 in school and at home:

* That people are not always who they say they are.
* That “Stranger Danger” applies to the people they encounter through the Internet.
* 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.

Year 7 pupils take part in the Bee Safe programme organised by the Magherafelt district council which encourages pupils to learn about safety online and in other situations.

# 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 to unsuitable materials or requests & ahat they should tell a teacher or trusted adult immediately

**Cyber Bullying**

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the schools overall anti -bullying policy and pastoral services as well as the e-Safety policy.

Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.

Cyber Bullying can take many different forms and guises including:

* Email – nasty or abusive emails which may include viruses or inappropriate content.
* Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
* Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user’s profile.
* Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
* Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
* Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person’s permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can **constitute a criminal offence**. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

* Protection from Harassment (NI) Order 1997
* http://www.legislation.gov.uk/nisi/1997/1180
* Malicious Communications (NI) Order 1988
* http://www.legislation.gov.uk/nisi/1988/1849
* The Communications Act 2003
* http://www.legislation.gov.uk/ukpga/2003/21
* It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

# Excessive Commercialism

The Internet is a powerful vehicle for advertising. In 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.

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

# **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.

# It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed **annually during Internet Safety Week.**.

# **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 encouraged to incorporate e-Safety activities and awareness within their lessons.

# **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.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use. Parents should remind their children about the SMART code which they have been taught in school. (See Appendix 4)

**Parental Advice:-**

* Only allow your child to use the internet in a particular room/area of your home where an adult can supervise.
* Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones, X box, Wii etc.
* 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. (See appendix2B)
* 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.

All staff in St. Mary’s Primary, take the issue of child safety very seriously. Since our duty to our pupils is paramount, we are conscious that any form of school publicity which involves the use of photographs must be carefully monitored. Therefore we wish parents to be aware of the following points:

* We ask for a parental consent forms to be signed so that photographs/videos of their children may be used in school, in the local press and on the School website/school Facebook page. (**Appendix 3)**
* Parents and guardians are permitted to take pictures of their family members during school activities i.e. Assemblies/ school productions. These photographs MUST be for personal use only and should not be displayed on social media sites i.e. Facebook without permission of those that are in the photographs

**Teaching and Learning**

# **Internet use:**

# The school 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/Internet Safety Week in February.

# 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 Child line/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.

# **E-mail:**

# Pupils may only use C2k e-mail accounts on the school system.

# Pupils must immediately tell a teacher if they receive offensive e-mail.

# 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.
* 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.
* Parents are advised not to post photos/videos of pupils on Social Networking sites.
* School staff are requested not to add children or Parents (with the Exception of work colleagues) as ‘friends’ if they use these sites. Parents and young people should not make this request of school staff.

**Mobile Technologies:**

* The use of portable media such as memory sticks and external hard drives will be approved by the teacher and will be closely monitored as potential sources of computer virus and inappropriate material.
* Staff should only store pupils’ personal data and photographs on encrypted memory sticks if they need to at all (supplied by school and must be returned and data deleted in the presence of a colleague when no longer a staff member)
* Pupils are not allowed to have personal mobile devices/phones in school at all. If a child should bring in such a device it will be automatically removed, locked in the school safe and a parent will have to come to the school to collect it.
* **Teacher I-pads need to have a pass code.**

**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, displays, school newsletters or any publication which the school deems appropriate etc. 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.
* Only Pupils’ first names will be used in association with photographs.
* Pupil’s work can only be published by outside agencies with the permission of the pupil and parents.
* Parents are aware of the images they take and where and when they use them. Posting images on to any Social Media Websites or using material without the permission of other parents is illegal and taken seriously by the PSNI.

**NB – Some parents may agree to** the school posting **their child’s image/video on the school facebook page but this does not automatically give other parent the right to post images taken/recorded at school events on any social media platform.**

**Policy Decisions:**

# **Authorising Internet access**

# Pupil instruction is responsible and safe and should precede any Internet access. 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 and must be reminded before each session.

# 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 must change periodically. Login details should not be shared with pupils.
* All pupils are provided with an individual login username and password.
* Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
* Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

**Handling e-Safety Complaints:**

* Complaints of Internet misuse will be dealt with by Mr Warnock (ICT Co-ordinator)
* 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 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/ Safeguarding Week/Internet Safety Week.
* 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’s 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 can be monitored and traced to the individual user. Discretion and professional conduct is essential.
* A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

**Monitoring and review:**

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors’ responsibility and they will review its effectiveness annually. They will do this through reviews conducted by the ICT Co-ordinator and Designated Child Protection Co-ordinator annually during Internet Safety Week.

**Appendix 1**

**Internet Safety: Staff Acceptable Use Policy**

# *As a professional organisation with responsibility for children’s safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school’s computer system in a professional, lawful and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.*

This version of the AUP was reviewed and amended in March 2019

by The Principal and Staff of St. Mary’s Primary School Greenlough

* I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, P.D.As., digital cameras, email and social media sites**.**
* School owned information systems and equipment must be used appropriately and I understand that it is the responsibility of the user to do so.
* I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff, including support staff.
* I will respect system security and I will not disclose any password or security information inappropriately.
* I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
* I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be used in a professional manner. Any images or videos of pupils will only be used as stated in the school Child Protection Policy.
* Any professional documents/data will be protected in a professional manner.
* I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
* I will respect copyright and intellectual property rights.
* I will report all incidents of concern regarding children’s online safety to the Designated Child Protection Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the I.C.T. Coordinator.
* I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Coordinator.
* Schools’ electronic communications with pupils, parents/carers, Board of Governors and other professionals will only take place via work approved communication channels e.g. via a school provided email address, telephone number or School’s Text Messaging Service. Any pre-existing relationships which may compromise this will be discussed with the Senior Management team.
* My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems.  This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
* I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school, into disrepute.
* I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
* If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the I.C.T. Coordinator or the Head Teacher.
* I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
* I will read/watch all internet publications fully before using with pupils in class.
* All staff will only use their own mobile phones or P.D.As. during pupil non-contact time or at designated breaks for personal use.
* All Permanent Teaching Staff, may use mobile phones or P.D.A.s for professional use and are responsible for the security of the device while it is on the premises.
* All Non-Permanent Teaching Staff, must seek prior permission from the Principal to use mobile phones or P.D.As for professional use. They are responsible for the security of the device while it is on the premises.
* All staff should not use personal E Mail Accounts to E Mail from on School I.C.T. equipment.

*The School may exercise its right to monitor the use of ~~i~~nformation systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School’s Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service’s information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.**

Signed: ……………………….... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………….

**Appendix 2A**

**Pupil Rules for Responsible Internet Use**

The school has installed computer and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

* **I will only use the computer for school work.**
* **I will not access other people’s files without permission.**
* **I will not use mobile/external storage devices.**
* **I will ask permission from a teacher before using the Internet.**
* **I understand that the school may check my computer files, e-mails and may monitor the Internet sites I visit.**
* **I will only e-mail people whom my teacher has approved.**
* **The messages I send will be polite and responsible.**
* **I will not give my home address or telephone number or arrange to meet someone.**
* **I will report any unpleasant material/message sent to me. I understand that my report would be confidential and would help protect other pupils and myself.**
* **I will only download information/files, which my teacher has permitted me to.**
* **I will not bring mobile phones or tablet computers to school.**
* I will only use the Internet when there is a teacher or another allocated person in the room.
* **If I do not abide by the above rules, my Internet privileges may be withdrawn.**
* **Pupil Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Year 3 Date \_\_\_\_\_\_\_\_\_\_\_\_\_**
* **Pupil Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Year 4 Date \_\_\_\_\_\_\_\_\_\_\_\_\_**
* **Pupil Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Year 5 Date \_\_\_\_\_\_\_\_\_\_\_\_\_**
* **Pupil Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Year 6 Date \_\_\_\_\_\_\_\_\_\_\_\_\_**
* **Pupil Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Year 7 Date \_\_\_\_\_\_\_\_\_\_\_\_\_**

St. Mary’s Primary School, Greenlough



**Internet Use Agreement for Pupils**

**Parent’s Consent Form**

# Introduction

Internet access is available for pupils in St. Mary’s. We feel that it will be of great benefit in enhancing pupils learning.

We also recognise the dangers associated with using the Internet and therefore the school has drawn up rules on the correct use of the Internet.

**The School:**

* Is seeking your permission for your child[ren] to access the Internet following the rules laid down by the school.
* Will use service provider (C2K), which is filtered to ensure the protection of the children from unsuitable materials. **( please note no filter is 100 % safe )**

**Please read the following agreement before signing:**

* The use of the school’s Internet account is a privilege and not a right.
* The school will deem what is acceptable use of the Internet.

## Internet Usage Consent Form

**Parent/Guardian**

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

**I accept the above paragraph**  **I do not accept the above paragraph**

*(Please tick as appropriate)*

In relation to the school website, I accept that, if the school considers it appropriate, my child’s schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing pupils’ work on the School’s website.

**I accept the above paragraph**  **I do not accept the above paragraph**

*(Please tick as appropriate)*

Pupil Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent / Guardian Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 3**

**St. Mary’s Primary School, Greenlough**

**CONSENT FORM FOR PHOTOGRAPHS AND VIDEO FOOTAGE**

[220, Mayogall Road, Portglenone, Co. Antrim]

Principal: Mr M Meehan (Principal)Telephone:12913

Website: stmaryspsgreenlough.com Email: [info@stmarysps.greenlough.ni.sch.uk](mailto:info@stmarysps.greenlough.ni.sch.uk)

**Consent Form** for .............................................................. Date of Birth ...............................

Photographs and recordings of pupils for School, family and press are a source of pride to both the pupils and their families//legal guardians. Taking, keeping and publishing photographs and video footage involves processing personal data under data protection laws.

To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain express consent to the use of a pupil’s image for example in school displays, performances, newsletters, prospectus and our social media platforms.

In all instances below, the image or footage may be of an individual, small group, class or classes. Where pupils are named, we will use first names only unless we have sought prior permission from you to publish full names (**\*newspaper and media companies will often use a full name and we will not seek further permission for this**). We will only use photographs and footage where pupils are appropriately dressed to reduce the risk of inappropriate use of the images or footage.

**A pupil aged 13 or over and who is considered capable of giving their own consent** can complete this form on their own behalf.

**Parents//legal guardians of pupils under the age of 13 or pupils over the age of 13 and not considered capable of giving their own consent** should complete this form on behalf of the pupil.

This consent form is valid for the academic years [ 2021 ] until your child leaves our school. Please inform us in writing if you wish to change your consent at any time. Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

* New requirements for consent, e.g. [an additional form of media to use with pupils/parents/legal guardians]
* Changes to school circumstances, e.g. [School Management reviews how the school markets itself]

|  |  |
| --- | --- |
| I give permission for photographs, voice recordings or videos of my child to be taken and used within school, for example: displays in school entrance. | Yes/No |
| I give permission for photographs of my child to be used in the printed school newsletter or posted in PDF format on the School website. | Yes/No |
| My child may be named (first names only) in the caption or article associated with the image in the school newsletter. | Yes/No |
| I give permission for photographs, voice recordings or videos of my child to be used on the School's website and our school-managed social media portals, for example: as part of a school trip blog. | Yes/No |
| I give permission for my child’s work to be used on the school website and our school-managed social media portals. | Yes/No |
| My child may be named (first name only) in the associated captions or articles on the website or school-managed social media portals. | Yes/No |
| My child’s image, voice or work may be used in school promotional materials, for example: prospectus, other publications that we produce for promotional purposes. | Yes/No |
| I give permission for visiting media organisations to take photographs or video footage of my child and use them in local or national publications, on websites and on radio or television programmes.  (If you wish to answer no to this question, and your child is selected (e.g. as a winner/participant in a competition, etc) we will present this option to you again, specifying the named local or national publication/website or tv provider. | Yes/No |
| My child's name\* may be used in connection with this material (visiting media organizations). (\*In these instances full names are often used). | Yes/No |
| My child may feature in footage recorded for the purposes of teacher training which is shared with other teachers in the school or externally to help raise teaching standards. | Yes/No |

* Please be aware that websites and social media can be viewed throughout the world and not just in the United Kingdom where UK law applies. Currently we do not have a social media account other than our website. We hope to introduce Twitter and / or Facebook. We will inform you appropriately when all is in place.
* We may continue to use your child's image or footage after they have left the School in promotional materials or on our social media or website accounts.
* We will not include personal e-mail or postal addresses, telephone or fax numbers on video, on our website or in any printed materials.
* We may include a pupil’s written work, projects and artwork including portraits of other pupils on our website and in promotional materials.

**Consent can be withdrawn at any time by notifying the Principal and completing a new copy of this form.** If you do not consent to a particular use of your (current pupil age 13+) or your child’s information, you/your child will not suffer any detrimental effect as a result.

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Principal. A new form will be supplied to you to amend your consent accordingly and provide a signature.

**For children aged under 13 or children aged 13 or over but not considered capable of giving their own consent:**

Signed by parent/legal guardian ......................................................

Print name .........................................................

Relationship to child .................................... Date ..................................................................

I am aware that if I take images or videos during a school event that posting these onto any Social media websites or using material without the permission of other parents is illegal and taken seriously by the PSNI.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Parent)

Dated: \_\_\_\_\_\_\_\_\_\_\_\_

### 

### **Appendix 4**

E-Safety Information for Parents/Carers

### **Safety Rules for Children**

#### Follow These SMART TIPS

**S**

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

**M**

**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.

**A**

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

**R**

**Remember** someone on-line may be 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!

**T**

**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

**TO BE DISPLAYED IN CLASSROOMS**

**Pupil Rules for Responsible Internet Use**

The school has installed computer and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

* I will only use the computer for school work.
* I will not access other people’s files without permission.
* I will not use mobile/external storage devices.
* I will ask permission from a teacher before using the Internet.
* I understand that the school may check my computer files, e-mails and may monitor the Internet sites I visit.
* I will only e-mail people whom my teacher has approved.
* The messages I send will be polite and responsible.
* I will not give my home address or telephone number or arrange to meet someone.
* I will report any unpleasant material/message sent to me. I understand that my report would be confidential and would help protect other pupils.

**Appendix 5**

**E-Safety Incident Log**

Date: \_\_\_\_\_\_\_\_

Name(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Class(es): \_\_\_\_\_\_\_\_\_\_

Teacher in charge: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Details of incident/issues + naming pupils involved directly & indirectly. |
| Synoposis of investigation & decisions taken in conjunction with Principal/ Class teacher/Child Protection Team. |
| Actions taken as a result.  E.g. Parent(s) informed, information shared with staff/ Anti-bullying / Positive Behaviour Policies invoked/PSNI informed. etc. |

Signed :- Teacher/Principal \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent’s signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Confidentiality – record filed in locked cabinet in Principal’s office and disposed in line with GDPR recommendations.)