# St Malachy's Primary School

# Digital Safety Policy & Acceptable Use Agreement

**Schedule for Developing, Monitoring and Reviewing Policy**

**Approval by the Board of Governors:**
Sept, 2024

**The implementation of this Online Safety policy will be monitored by:**
The Online Safety Coordinator

**Monitoring and reviewing:** Sept 2025, and only if required following a breach of safety.

**Should serious Online Safety incidents take place, the following external persons or agencies should be informed:**
PSNI, Chair of BoG and EA

September 2024

**Table of Contents**

## 1. 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 and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Apps
- Mobile/Smart phones with text, video and/or web functionality
- Ipads, tablets and 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.

This policy, supported by the school's Acceptable Use Agreement (see appendix) 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, Safeguarding, and Anti-bullying compliant with 'The addressing Bullying in Schools Act (NI 2016). It has been agreed by the School Leadership Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

## 2. Rationale

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

*DENI Online Safety Guidance, Circular number 2016/27*

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

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

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

In relation to Online Safety incidents that occur outside of school hours, the School will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. Online Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of Online Safety incidents outside of the School, will be dealt with in accordance with School Policies.

**4. Risk Assessment**

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

The main areas of risk for the School can be categorised as the Content, Contract and Conduct of activity.

**1. Content**

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

**2. Contact**

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

**3. Conduct**

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

Many of these risks reflect situations in the offline world and it is essential that this Online Safety policy is used in conjunction with other School policies e.g. Positive Behaviour, Safeguarding , Anti-Bullying and Acceptable Use, Mobile devices and Disposal of documents.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

## 5. Roles and Responsibilities

### 5.1 Online Safety Coordinator

The Online Safety Coordinator will lead the Online Safety Committee and takes day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

The Online Safety Coordinator will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provide training and advice for staff
- Liaise with C2K
- Liaise with the EA and DENI on Online Safety developments
- Receive reports of Online Safety incidents and create a log of incidents to inform future Online Safety developments
- discuss current issues, review incident logs
- monitor and report to staff any risks to staff of which the Online Safety coordinator is aware

### 5.2 Online Safety Officers / Designated Child Protection Officer / Designated Deputy Child Protection Officer

The Child Protection Officer (C Donnelly) and their deputy (C Kearney) will be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

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

### 5.3 Online Safety Committee

The Online Safety Committee provides a consultative group with responsibility for issues regarding Online Safety and the monitoring of the Online Safety policy including the impact of initiatives.

Committee Members:

- Online Safety and ICT Coordinator : Mrs C. Connolly
- School Principal : Mr P. Duggan
- The Child Protection Officer : Mrs C Donnelly
- E- Safety Staff Representative : Mrs C Kearney (Vice-Principal)

Members of the Online Safety Committee will assist the Online Safety Coordinator with:

- The production and review of the school Online Safety policy and related documents.
- mapping and reviewing the Online Safety curricular provision, ensuring relevance, breadth and progression
- monitoring incident logs
- consulting parents/carers and the pupils about the Online Safety provision

**5.4 The Principal and Senior Leadership Team:**
The Principal has a duty of care for ensuring the safety (including Online Safety) of members of the school community though the day-to-day responsibility for Online Safety will be delegated to the Online Safety Officers.

The Principal and Online Safety Officer will be kept informed about Online Safety incidents.

The Principal will deal with any serious Online Safety allegation being made against a member of staff (refer to the Safeguarding policy).

The Principal and SLT are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

**5.5 Governors:**
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports.

**5.6 Network Manager - Mrs Cathy Connolly**
The Network Manager will monitor that C2K Online Safety measures, as recommended by DENI, are working efficiently within the school.

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

**5.7 Teaching and Support Staff**
The Teaching and Support Staff are responsible for ensuring that:
- They have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- They have read, understood and signed the school's Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the Online Safety Coordinator.
- Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School's guidance.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Staff understand and follow the school Online Safety Policy and Acceptable Use Policy.
- That students have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998)
- They monitor ICT activity in lessons, extracurricular and extended school activities.

- They are aware of Online Safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- Undertake all Online Safety training as organised by the school

**5.8 Professional Development for Teaching and Support Staff**

Training will be offered as follows:

- All new staff will receive Online Safety training, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.
- A programme of Online Safety training will be made available to staff as an integral element of CPD. Training in Online Safety will be supported within the PRSD or EPD process and where staff have identified a need.
- Staff will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings.

**5.9 Pupil Online Safety Committee (Digital Leaders)**

The pupil Online Safety committee (Digital Leaders) will assist the Online Safety Officers with:

- Potential issues regarding Online Safety
- Present information during assembly on Safer Internet Day.
- Present information on the school's monthly rules for internet safety at assemblies.

**5.9.1 Pupils**

Pupils are responsible for ensuring that:

- They use the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to schools systems.
- They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They know and understand school policies on the use of mobile phone, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Pupils are introduced to email and taught about the safety and 'netiquette' of using e-mail both in school and at home
- They understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

**5.9.2 Online Safety Education for Pupils**

Online Safety education for student will be provided in the following ways:

- A planned Online Safety programme (Online Safety with Cyber Tiger) will be provided as part of ICT / PDMU / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources and 'Be Internet Legends' will be used as a teaching tool.
- Pupils will be taught in all relevant lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.

- Pupils will be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils will be made aware of the school's monthly rules for internet safety.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

### 5.9.3 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the Online Safety policy outlined by the School.

Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- online communication with staff
- their children's personal devices in the school

### 5.9.4 Parents / Carers Training and Support

Parents and carers have essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and carers through:
- Parent workshops.
- A section of the school website will provide links to external sites such as CEOP
- Online Safety Guidance will be delivered through key events

### 5.9.5 Education for the Community

- The school will provide opportunities for members of the community to gain from the school's Online Safety knowledge and experience through:
- The school website
- Supporting community groups e.g. library staff/sports/voluntary groups to enhance their Online Safety provision
- Supporting other local schools and communicating with them to mutually enhance Online Safety provision.

## 6. Current Practice

### 6.1 Communication

- The official school email service may be regarded as safe and secure. Staff and pupils should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Email communications with parents and/or pupils should be conducted through the following school email systems '@c2kni.net' Personal email addresses should not be used.

- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers - email, Seesaw and official school social media accounts - must be professional in tone and content. When emailing, staff should CC any communication to pupils to another member of staff.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

- Further information is provided to staff during in service training, also see the 'Acceptable Use Policy' for appropriate use.

### 6.2 Social Networking

At present, the school endeavors to deny access to social networking sites to pupils during school hours. Staff may use You Tube and Seesaw to disseminate information to pupils.

- Teachers should adhere to the social networking / communication guidance provided by the school.
- Teachers and pupils should report any incidents of cyber-bullying to the school.

### 6.3 Pupils' use of personal devices

- Children may take mobile phones to school, but they must be switched off and remain in their school bag during school hours.
- If this is not followed, the mobile phone will be confiscated and kept in the Principals office until home time, where it will be collected by a parent.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- Where staff members are required to use a mobile` phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Further information is provided to staff/pupils/parents during in service training, also see the 'ICT Policy' for appropriate use.

**6.4 CCTV**

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission, except where disclosed to the Police as part of a criminal investigation.

**6.5 Digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

- When using digital images, staff informs and educates pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. Social Networking websites.
- The school gains parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those image.
- We will also ensure that when images are published that the young people cannot be identified by the use of their names, unless prior consent has been obtained.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- The use of digital / video images plays an important part in learning activities.
- The school will comply with the General Data Protection Register (introduced May 2018) by requesting parents' permission when their child starts school Year 1, permission will last until the student leaves school, unless a parent / carer provides a written withdrawal of taking images of members of the school.

**6.6 Teaching and Support Staff: Password Security**

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

- Staff are expected to have secure passwords which are not shared with anyone.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.

**6.7 Students: Password Security**

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Acceptable Use Policy
- Students are expected to keep their passwords secret and not to share with others, particularly their friends.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

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

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

**6.9 The Data Protection Act**
The school has a Data Protection Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they:

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

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

- the device is password protected
- the device offers approved virus and malware checking software
- the data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete

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

**They manage the school filtering by:**

- Monitoring reports of the use of C2k is available on request.
- Keep records and logs of changes and of breaches of the filtering systems.
- These changes and breaches should be reported to the Online Safety Coordinator.

**Staff and pupils have a responsibility:**

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

**Auditing and reporting:**

Logs of filtering change controls and of filtering incidents will be made available to:

- Online Safety Committee
- Online Safety Coordinator
- Board of Governors
- External Filtering provider / Police on request

**8. Managing Incidents**

- 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, Mrs Connolly.
- 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 Safeguarding procedures.
- Pupils and parents will be informed of the complaints' procedure. (Ref. CCMS complaints procedure)
- Sanctions for the misuse of technology are outlined in the Acceptable Use Policy:
- Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Anti-Bullying Policy will be implemented.

**9. Communicating the Policy:**

**Introducing the e-Safety Policy to pupils**

- e-Safety rules will be displayed in all classrooms and discussed with the pupils.
- Specific lessons will be taught by class teachers regularly e.g. during ICT and PDMU lessons/circle times/anti-bullying week/Internet safety day.
- Pupils will be informed that network and Internet use will be monitored**.**
- A visual aid (Tony the Cyber Tiger) will be used to reinforce SMART safety rules
- Each month the school will focus on one Internet Safety Rule (see appendix)
- The Digital Leaders will assist in reinforcing SMART safety rules and the monthly rules.

**Staff and the e-Safety Policy:**

- All staff will be given the School e-Safety Policy and its importance explained in August of each year with the Safeguarding training.
- 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 or tablet 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.

**10. 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.

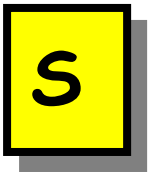
**11. Appendix**

See the Appendix for:

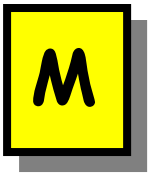
- SMART rules for internet safety.
- Tony the Cyber Tiger.
- Monthly rules for internet safety.
- Acceptable Use Agreement for Pupils.
- Acceptable Use Agreement for staff.

**Safety Rules for Children**

Follow These SMART TIPS



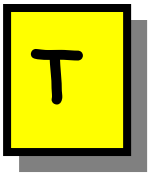

**Secret -** Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!




**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.


SAFE
Keep your personal information safe
MEET
Friends made online are strangers; meeting them can be dangerous
ACCEPTING
Accepting files can be dangerous. If unsure, ask an adult!
RELIABLE
Not everyone or everything online is reliable or trustworthy
TELL
Always tell an adult if something online upsets or annoys you.
CYBER TIGER

# St Malachy's Primary School Month Internet safety rules

**September - Never give away personal information**

Keep your private information private. Never give out you name, address or school name – use a made up name.

**October - The internet is forever**

Before posting a photo or sending a message via the internet, ask yourself if you are okay with everyone in the world seeing it. Clearing your history or deleting a post does not necessarily make your actions disappear.

**November - Don't trust strangers**

Always treat anyone you meet on the internet as strangers, regardless of how long you have chatted or how well they think they know them. Never meet up with a stranger.

**December - Make passwords long and complex**

Create long and complex passwords to protect your accounts.

Christmas Internet Safety tips

**January - Report bad activity and don't respond**

If someone behaves inappropriately to you on the internet, then you should report it to an adult immediately. An adult can block the user and report them to the website or game.

**February - Treat others as you want to be treated**

This golden rule applies to real life and the internet. Use the internet to support, teach, and inspire. Before you post remember to THINK.. Is it True, Helpful, Inspiring, Necessary or Kind. If not don't post it!

**March - Don't buy things without permission**

You must ask permission before making an online purchase. Be careful of what you click on especially in games.

**April - Don't download or explore without permission**

Don't download or explore without permission. Use Kiddle as a search engine to provide kid-friendly results.

**May – Talk**

Talk to your trusted adult and set up rules for going online. Decide upon the time of day and the length of time that you can be online. Decide appropriate areas for you to visit and things for you to do.

**June - Take a break!**

Humans were not designed to sit in front of the computer for extended periods of time. Using the computer for a long time can hurt your wrists, back, eyes, and brain. Take a break from screen and go outside to play.

## An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.

I

- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
- I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/cares will be informed.

**Our PRIMARY SCHOOL**

Acceptable Use Agreement
For Pupils

Please complete and return this form to your child's class teacher

| | | | |
|---|---|---|---|
| **Pupil's Name** | | **Class Teacher** | |
| As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school. | | | |
| **Pupil Name (print)** | | | |
| **Pupil Signature** | | **Date** | |

| | | | |
|---|---|---|---|
| **Parents Name** | | | |
| As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information. | | | |
| **Parents Name (print)** | | | |
| **Parents Signature** | | **Date** | |

**ST. MALACHY'S PRIMARY SCHOOL**

Acceptable Use Agreement
For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

| **Name** | | |
|---|---|---|
| **Date** | | **Signed** |