

# Killowen PS Rostrevor



## E-Safety/Online Safety Policy

*Faith, Friendship and Understanding*

Agreed by Governors	
Review Date	
Principal	
Chair of Governors	

## Mission Statement

### Aims

**In Killowen Primary School:**

- We aim to enable excellence so that pupils develop to their full potential academically, personally and spiritually and become determined, independent, life-long learners who make meaningful contributions to the world.
- We aim to foster a nurturing, inclusive environment where kindness, resilience, empathy and faith guide every interaction and where every individual feels valued and respected as part of our school family.

### Mission

**In Killowen Primary School, we believe we can achieve our aims by ensuring we are committed to:**

- Promoting the values of Catholic education within our school family
- Having high expectations for all pupils and a desire to see them reach their full potential
- Having inclusive, stimulating and supportive classrooms
- Working together for a common goal
- Valuing continuous improvement for all
- Investing in people and resources
- Working closely with home and the wider community

### Values

- Kindness
- Respect
- Resilience
- Equality
- Unity
- Determination
- Excellence
- Empathy
- Trust

# Introduction

In line with recent guidance from the Northern Ireland (NI) government on safeguarding children and young people in the digital environment, Killowen Primary School recognises the importance of embedding e-safety into our school culture. This policy aims to provide a framework for the responsible and secure use of Information and Communications Technology (ICT), both inside and outside the classroom.

The ICT resources children are currently using include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email, Instant Messaging, and Online Collaboration Tools
- Social Networking, Blogs, Wikis
- Video Broadcasting, Podcasting, and Media Sharing
- Gaming and Streaming Services
- Mobile/Smart Devices with web functionalities

We recognise the benefits of these technologies for education and learning but are equally aware of the potential risks. This e-safety policy is designed to educate pupils on safe online practices while fostering digital literacy, critical thinking, and responsibility.

## Aims and Objectives

The primary aim of this policy is to ensure that all pupils, staff, and parent(s)/Carer(s) are aware of their responsibilities regarding e-safety. We aim to:

- Equip children with the knowledge to use the internet and digital technologies safely and responsibly.
- Promote a positive culture of online safety and responsible digital citizenship.
- Ensure appropriate measures are in place to protect pupils from risks associated with digital technology.
- Collaborate with parents, staff, and external agencies to support children in staying safe online.

# Key E-Safety Risks

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 communication 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:

## 1. Potential Online Contact

Children may encounter individuals who seek to exploit or harm them. We aim to teach children:

- Not to disclose personal information such as names, addresses, or phone numbers online.
- That individuals online may not always be who they claim to be.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- Never to meet in person someone they have only met online without a trusted adult present.
- That once they publish information it can be disseminated with ease and cannot be destroyed.

## 2. Inappropriate Content

Children may come across content that is unsuitable or harmful, including violent, sexual, or extremist materials. We will ensure children are taught:

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

### **3. Cyberbullying and Harassment**

Cyberbullying is a serious issue that can affect the well-being of children. Pupils will be educated on how to:

- Recognise cyberbullying.
- Seek help from trusted adults or organisations if they experience or witness bullying online.

### **4. Data Privacy and Security**

Children must understand the importance of safeguarding their personal data online. We will instruct them to:

- Use secure passwords and understand the importance of keeping login information private.
- Be cautious about sharing personal information and refrain from filling in unnecessary online forms.
- Not to use an adult's credit card number to order online products.

### **5. Excessive Screen Time and Gaming**

Unmonitored access to online gaming and excessive screen time can lead to unhealthy habits. Pupils will be encouraged to:

- Balance online activities with other healthy pursuits and limit recreational screen time.
- Avoid playing age-inappropriate games and report inappropriate gaming interactions.

## **Roles and Responsibilities**

### **1. Governors and Leadership**

The Principal and Board of Governors have the ultimate responsibility to ensure the e-safety policy is effectively implemented and reviewed regularly. This includes:

- Ensuring all staff receive regular e-safety training.
- Reviewing the policy annually and ensuring its alignment with NI guidelines and CEOP (Child Exploitation and Online Protection) resources.

## **2. ICT Coordinator**

The ICT Coordinator will lead the school's efforts to maintain a safe digital environment by:

- Keeping updated on the latest e-safety guidelines.
- Conducting regular e-safety awareness sessions for staff and pupils.
- Overseeing the school's filtering and monitoring systems.

## **3. Teachers and Support Staff**

Teachers are responsible for embedding e-safety practices in daily learning and ensuring that:

- Pupils are aware of safe practices when using the internet and technology.
- E-safety is integrated into the curriculum through age-appropriate activities.
- They report any breaches of e-safety policy or incidents involving inappropriate online behaviour.

## **4. Pupils**

Pupils are expected to follow the e-safety guidelines, including:

- Keeping their personal information secure.
- Reporting any uncomfortable or inappropriate content they encounter online.
- Understanding and following the school's Acceptable Use Agreement (Appendix 1)

## **5. Parents and Carers**

Parent(s)/Carer(s) play a critical role in ensuring e-safety at home. They should:

- Monitor their child's online activities and screen time.
- Set clear rules for responsible internet use at home.
- Discuss e-safety tips with their children, including the SMART rules (Appendix 2)

## **Teaching and Learning**

### **1. E-Safety Curriculum**

- E-safety lessons will be planned across all year groups and integrated into various curriculum areas.
- Pupils will be taught about the dangers of the internet, how to protect themselves, and the responsible use of digital tools.
- Specific lessons will cover topics such as cyberbullying, online privacy, and the safe use of social media.

### **2. Safe Use of Internet Resources**

- All internet use will be supervised, and filtering systems will block inappropriate content.
- Pupils will be taught to critically assess online information for accuracy and reliability.
- The use of online resources will be tied to educational objectives, with aimless browsing discouraged.

# **E-Safety for Staff**

## **1. Staff Training**

All staff will receive annual training on e-safety procedures, including:

- Safe use of the internet and school systems.
- Handling incidents of inappropriate or illegal online behaviour.
- Ensuring that personal data is handled securely.

## **2. Staff Responsibilities**

- All staff must adhere to the Acceptable Use Agreement and ensure that pupils follow the e-safety rules. (Appendix 3)
- Internet activity must be for professional purposes, and staff must avoid accessing or sharing inappropriate content.

# **Working with Parents**

## **1. Parent Engagement**

We will engage with parents by:

- Providing e-safety information through newsletters, workshops, and our school website/Facebook.
- Encouraging parents to support e-safety practices at home and maintain open dialogue with their children about online activities.

## **2. Parental Consent**

Parents will be required to sign the Acceptable Use Agreement for their children and will be informed about how the school uses pupil data and images online.

## **Handling E-Safety Complaints**

- Any complaints or breaches of e-safety will be dealt with by
- Incidents involving safeguarding concerns will be reported to the Designated Child Protection Teacher and handled according to child protection procedures.
- Pupils and parents will be informed of the complaints procedure and encouraged to report concerns.
- 

## **Monitoring and Reviewing**

This policy will be reviewed annually by the ICT Coordinator and the Designated Child Protection Teacher, with oversight from the Board of Governors. Regular audits will be conducted to assess the effectiveness of the policy and its implementation.

## **Conclusion**

At Killowen Primary School, we are committed to creating a safe digital environment for our pupils. By educating children, staff, and parent(s)/carer(s), we aim to ensure that all members of our school community can enjoy the benefits of technology safely and responsibly.

## Appendix 1

### **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-mails 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-mails, 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 receive messages I do not like, I will tell a teacher immediately.
  - I will not bring in memory sticks 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.

**Killowen Primary School**

**Acceptable Use Agreement  
For Pupils**

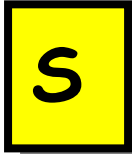
Please complete and return this form to your child's class teacher.

<b>Pupil's Name</b>		<b>Class Teacher</b>	
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.			
<b>Pupil Name (print)</b>			
<b>Pupil Signature</b>		<b>Date</b>	

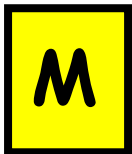
<b>Parents Name</b>			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable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

## 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

### Appendix 3

#### **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.

<b>Name</b>		
<b>Date</b>		<b>Signed</b>

