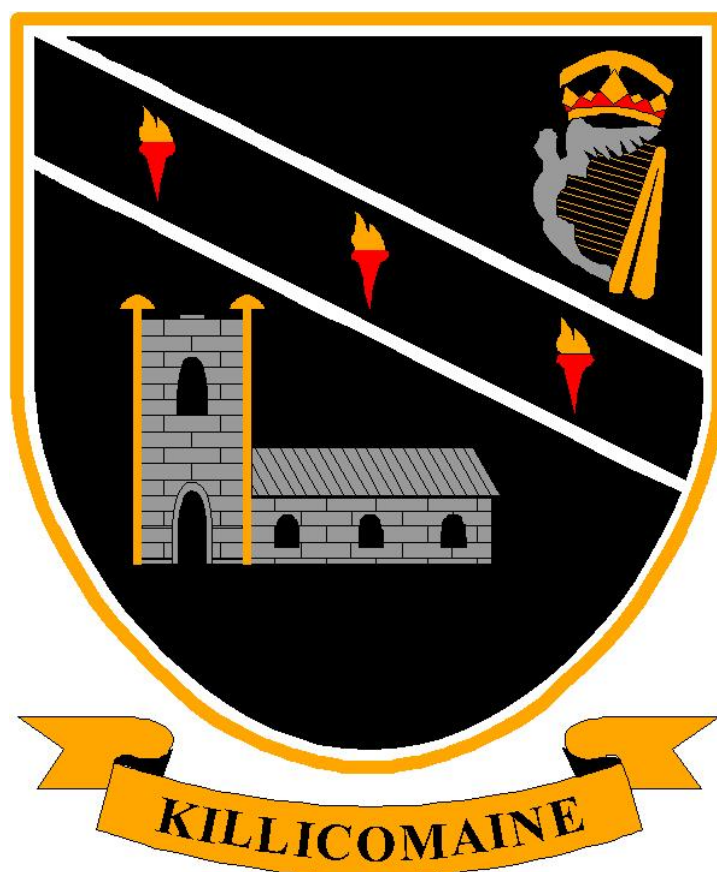


Killicomaine Junior High School

E-SAFETY POLICY & ACCEPTABLE USE AGREEMENT



**“Working together for excellence
within a caring community”**

INTRODUCTION

We, in KJHS recognise the requirement to ensure that pupils are able to use the internet and related communications technologies appropriately and safely. This is addressed as part of the wider duty of care to which all who work in our school are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

New technologies have become integral to the lives of our pupils and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Our pupils should have an entitlement to safe internet access at all times.

There is lots of evidence that recognises the benefits that the use of digital technologies can bring to teaching and learning. We aim to teach our pupils 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.

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 school, include:

- Websites
- Learning Platforms – G Suite, VLEs
- 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 eg. Ipads, kindles

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

THE INTERNET

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key Concerns are:

POTENTIAL CONTACT

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

- That people are not always who they say they are.
- That "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.

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 will be taught:-

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

EXCESSIVE COMMERCIALISM

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

Children will 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 to keep abreast of current e-safety issues and guidance through organisations such as *CEOP* (Child Exploitation and Online Protection), *Childnet* and *CBBC Web Stay Safe*.
- The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.
- The ICT Co-ordinator update Senior Management and Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

ASSESSING RISKS

- The school will take all reasonable precautions to prevent access to inappropriate material.
- However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

E-SAFETY INFORMATION FOR PARENTS/CARERS

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website contains useful information and links to sites like CEOP's, Childnet, and the CBBC Web Stay Safe page.
- The school will communicate relevant e-Safety information at the beginning of the school year in the 'Key Points for Internet Safety Leaflet' (appendix 3), through newsletters and the school website.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

LEARNING AND TEACHING

INTERNET USE:

- The school will plan and provide opportunities within a range of curriculum areas to teach online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

EMAIL

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- The network administrator will make the decision to release filtered emails based on their content
- The forwarding of chain letters is not permitted.

PUBLISHING STUDENTS' EMAIL AND WORK

- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents/carers.

SOCIAL NETWORKING

- Students are unable to access social networking sites such as Facebook and Twitter through the C2K network.
- Teachers who learn of students accessing social networking sites via a 'backdoor' should alert the ICT coordinator or ICT technician immediately to have the site banned.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

MOBILE TECHNOLOGIES

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile devices/phones (in school) during class.

MANAGING VIDEO CONFERENCING:

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

POLICY DECISIONS

AUTHORISING INTERNET ACCESS

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.

PASSWORD SECURITY

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

HANDLING E-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- 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.
- Students and parents will be informed of the complaints procedure.

COMMUNICATING THE E-SAFETY POLICY

INTRODUCING THE E-SAFETY POLICY TO PUPILS

- Safety rules will be posted in all rooms where computers are used. (Appendix 4)
- Specific lessons will be taught by ICT teacher at the beginning of every year and at relevant points throughout the year.
- Students will be informed that network and internet use will be monitored.

STAFF AND THE E-SAFETY POLICY

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations.
- Staff must take care always to maintain a professional relationship.

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.

E-SAFETY INFORMATION FOR PARENTS/CARERS

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child. (Appendix 1)
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school will communicate relevant e-Safety information through internet and safety leaflet, newsletters and the school website.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips. (Appendix 3&4)
- 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.

Implementation Date: 2019/2020

Review Date: This policy will be reviewed academic year 2022/2023

APPENDIX 1

COMMUNICATION WITH PARENTS/CARERS RE ELECTRONIC DEVICES

Dear Parent,

Computer and Internet Use

As part of the schools ICT programme, we offer pupils supervised access to our computer network and the Internet, to give them the opportunity to develop their ICT skills. The Internet is an increasing feature of everyday life but along with its benefits the Internet also brings risks.

To protect pupils, our Internet service provider performs rigorous filtering of the World Wide Web and electronic mail for inappropriate and offensive material. Nevertheless you should be aware that the potential to access inappropriate material does exist and that no filtering technology can completely guarantee that a pupil will never come across distasteful material in some form or other.

Before being allowed to use the school network and access the Internet, all pupils will be required to agree to and sign the school's ICT Acceptable Use Statement (copy enclosed). The school needs your support in expecting pupils to use their access to the school network and the Internet in a responsible manner at all times. You are therefore asked to counter-sign the Acceptable Use Statement completed by your son/daughter to confirm your approval and their acceptance of the school rules on this matter.

Yours sincerely,

W Radcliffe / S Orbinson

ICT Coordinator

.....

Principal

Acceptable Use Guidelines of the Computer & Internet for Pupils

ICT ACCEPTABLE USE

- 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 use the Internet for research and school purposes only.
- I will ensure that any e-mails I send are polite, sensible and responsible.
- I will only send e-mails which my teacher has approved. I will not forward chain letters or insulting emails
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When using the internet and sending e-mails I will protect myself and others by not giving out my name, address, phone number, photo or other personal information about yourself and others
- I will not arrange to meet any online contact. I will tell my teacher about any invitations to meet on-line contacts
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- I will tell a teacher if I see web pages or e-mails which are offensive or unpleasant.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I will only access the Internet for educational purposes and not for advertising, gambling or political purposes.
- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce. (Copyright legislation)
- I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/carers will be informed.

Pupil Name:

Pupils Signature: Date

Parent's Signature:Date

APPENDIX 2

August 2013

Dear Parent/Person with parental responsibility,

To save you having to fill in permission slips for all the individual activities, outings and events which take place throughout the school year we have included them all in this one letter. Please read each carefully, then *delete* where appropriate, *sign* and *return* to your child's Form Teacher on the first day back to school.

Yours sincerely

Principal

SCHOOL OUTINGS

Throughout the year your child will be participating in a variety of projects outside school. These may include sporting events, choir singing and visits to places of educational interest etc. You will be informed of any visits and the relevant dates by the Head of Department.

CHILD'S NAME: _____ CLASS: _____

I give / do not give* permission for my child to attend school outings in the school year 2012/13.

Signed: _____ (parent/guardian) Date: _____

PHOTOGRAPHS & FILMING

Photographs of your child may be used in school on display boards, in the school magazine or in local newspapers' after competitions or sports events etc. They may also be used on the school website to show things which are happening in school.

CHILD'S NAME: _____ CLASS: _____

I agree / do not agree* that photographs of my child may be used for displays, on the school website, school magazine and in the local press.

Signed: _____ (parent/guardian) Date: _____

(* delete as appropriate)

INTERNET USE (Year 8 pupils only)

Killicomaine Junior High School produce an Internet Acceptable Use Policy. This policy is to ensure that the internet is used safely by pupils and staff. In order to ensure that you and your child agree with the rules on the use of the internet in school please sign in the relevant place below. Failure to sign the form below will result in your child not being allowed to use the internet in school.

Pupil

As a school user of the Internet, I agree to comply with the rules on its use. I will use the school network in a responsible way and observe all the restrictions explained to me by the school.

Signed: _____ (Pupil's signature) Date: _____

Parent

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.

Signed: _____ (Parent's signature) Date: _____

CEIAG

Killicomaine Junior High School has a Careers Service Partnership Agreement with the Careers Service NI which ensures your son/daughter has access to high quality Careers Education, Information, Advice and Guidance.

To offer CEIAG, the Careers Service needs basic information about pupils (name, address, date of birth, special needs/disability and school attended). We require your permission to share this information with the Careers Service. This information will only be used for careers guidance, will be securely stored and security conforms to all requirements under the Data Protection Act 1998. It will not be supplied to third parties but may be used in anonymous form for statistical analysis.

CHILD'S NAME: _____ CLASS: _____

I give / do not give* permission for my child's information, as listed above, to be shared with Careers Service NI.

Signed: _____ (parent/guardian) Date: _____

APPENDIX 3

Killicomaine Junior High School

Key Points for Internet Safety



The Smart Rules for Internet Safety are:



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.

Our full e-Safety Policy is available from the office

What is the Internet?

The Internet is a huge network of computers making a worldwide community. It is a way of connecting computers together so that people using them can:

- Talk to each other and have fun
- Send and receive messages
- Obtain information and resources
- Publish information
- Buy and sell things

Why do we use the Internet in school?

The Internet is a unique and exciting resource. It brings the world into the classroom. It has many educational benefits:

- It gives children opportunities to find up to date information that might otherwise be unavailable in school
- It provides fast and efficient communication
- It encourages independent learning and children enjoy using it
- Use of the Internet is an essential skill for children as they grow up in the modern world

What are the Dangers for my Child using the Internet?

The Internet is available to all. This can bring young people into contact with unsuitable persons. Children should be taught:

- People they encounter on the Internet are not always who they say they are
- That they should never give personal details to a stranger on the Internet
- That they should never meet alone anyone contacted via the Internet

Some material on the Internet can be inappropriate for children as it may contain unsuitable information or images. Children need to know how to respond to unsuitable materials or requests on the Internet. They should be taught:

- To tell a teacher or an adult immediately if they find unsuitable material
- To tell a teacher or adult immediately if they are requested to do something that makes them feel worried and/or uncomfortable

What can we do in School?

In our school we do everything we can to protect children using the Internet:

- All access to the Internet is provided through a filtered service
- Internet use is supervised by an adult
- Children discuss and investigate Internet Safety issues as part of their PDMU programme.
- Children are taught Internet Safety rules (see overleaf)



What can you do at Home?

It is important to promote Internet Safety in the home and to take an interest in what your children are doing on the Internet.

- Keep the computer in an area of your home where you can see your child using it.
- Know which technologies (mobile phones, Gaming devices) provide internet access and discuss their use with your child.
- Keep an eye on the clock! Too much time spent on the Internet can be unhealthy
- Remind children that there are websites which are unsuitable. If they come across unsuitable materials, they must tell you.
- Know the SMART rules for Internet safety and discuss them with your children.

APPENDIX 4

THE SMART RULES FOR INTERNET SAFETY

Follow These SMART TIPS

