

Clare Primary School



E-Safety Policy and Acceptable Use Agreement

Date the policy came into effect	January 2019
Date of next policy review	January 2021
Name of person responsible for this policy	ulCT Co-ordinator, Safeguarding Team, Principal, BOG & staff
Other related policies	Behaviour and Citizenship, T&L, Pastoral Care, Anti-bullying, Safegaurding, ICT
Issued to	Staff, BoG, Parents (pupils)

2018/2019

Revised January 2019

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
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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

In Clare Primary School we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them 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.

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.

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, bulimia or self-harming.

Children should be taught:-

- To seek adult permission before using a device connected to the internet
- 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 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 to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety curriculum throughout the school.

The Principal/ICT Co-ordinator will 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.

The Safeguarding Team are responsible for maintaining a register of all reported e-safety incidents.

An ICT Register of Access is held and will be updated annually each January, outlining the access of staff members to specific systems, files and folders (APPENDIX 1).

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, Safe Guarding, 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 regularly.

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 will facilitate class participation in Internet Safety Day and teach e-safety skills throughout the year.

E-Safety Information for Parents/Carers

- All parents will receive a Trifoldleaflet regarding e-safety within school with helpful advice and sources of information (revised January 2019). (APPENDIX 2)
- 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 within school, on the school website and/or for use .in internal or external publicity.
- The school website contains useful information and literature containing links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page were distributed to all parents.
- The school will communicate relevant e-Safety information through newsletters and the school website.

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

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

Teaching and Learning

Internet use:

- 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.
- 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.

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 for most users.
- Social Networking will only be made available via C2K to those having completed the relevant forms.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Mobile Technologies:

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

Managing Video-conferencing:

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

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Photographs of individual pupils will not be permitted without parental consent. Only pictures of groups or group activities will be used.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms (APPENDIX 3).
- 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 (APPENDIX 4).
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource (APPENDIX 5).

Password Security:

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

Handling e-Safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Designate teacher in the E-Safety Register.
- 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 Safe Guarding Policy.
- Pupils and parents will be informed of the complaints' procedure.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored.

.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop 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 regularly. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

Signature _____

Signature _____

	Areas				Resources
Year Group	Potential Contact	Inappropriate Content	Excessive Commercialism	Conduct On-line	
Year 1	<ul style="list-style-type: none"> What is a stranger? How do we treat them? 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. We should ask permission to use devices and go on-line. 	<ul style="list-style-type: none"> We can buy things on-line. 	<ul style="list-style-type: none"> How bullying can effect emotions and self-esteem. 	<ul style="list-style-type: none"> DigiDuck e-book for young children
Year 2	<ul style="list-style-type: none"> Who is in our community? How do we connect with our community using technology? 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. We can talk to a grown up about the things we see and hear on-line. 	<ul style="list-style-type: none"> When we buy goods on-line we use real money. There are advertisements on-line to encourage us to want things. 	<ul style="list-style-type: none"> How bullying can effect emotions and self-esteem. Be respectful of both off-line and online communities as a way to learn to be good digital citizens. 	<ul style="list-style-type: none"> DigiDuck e-book for young children
Year 3	<ul style="list-style-type: none"> People are not always who they say they are. Stranger Danger applies to the internet / on-line gaming forums. 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. To understand that not everything on the internet is good for you. 	<ul style="list-style-type: none"> There are advertisements on-line to encourage us to want to buy things. You-tubers can try to persuade us to want items. 	<ul style="list-style-type: none"> Be respectful of both off-line and online communities as a way to learn to be good digital citizens. 	<ul style="list-style-type: none"> The Adventures of Smartie the Penguin
Year 4	<ul style="list-style-type: none"> Passwords are private information and should not be shared. Never meet anyone contacted through the internet. 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. That information on the Internet is not always accurate or true. 	<ul style="list-style-type: none"> We should never to use an adult's credit card number to order online products. We understand that some sites exist to encourage people to buy products 	<ul style="list-style-type: none"> How to respond if they discover instances of on-line bullying Explore the differences between in person and on-line communication and learn how to write respectful messages. Why do people use passwords and how can we create strong passwords. 	<ul style="list-style-type: none"> Cara Winston and the SMART Crew and video
Year 5	<ul style="list-style-type: none"> Be careful how you use / share both your own and others' personal details. Never meet anyone contacted through the internet. 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. That information on the Internet is not always accurate or true. 	<ul style="list-style-type: none"> We should never to use an adult's credit card number to order online products. We understand that some sites exist to encourage people to buy products 	<ul style="list-style-type: none"> Children can act like bullies online. Explore what cyber bullying means and what they can do when they encounter it. How to respond if they discover instances of on-line bullying Why do people use passwords and how can we create strong passwords. 	<ul style="list-style-type: none"> Jigsaw Video
Year 6	<ul style="list-style-type: none"> Once we publish content it is easy to share and hard to remove e.g. video's and photographs Never meet anyone contacted through the internet. 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. To question the source of information. How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately. 	<ul style="list-style-type: none"> We should never to use an adult's credit card number to order online products. We should not fill out forms with a lot of personal details. 	<ul style="list-style-type: none"> Information put on line leaves a digital footprint or trail, this can be big or small, helpful or hurtful depending on how they manage it. Protect yourself from identity theft by how we share information 	<ul style="list-style-type: none"> Jigsaw Video
Year 7	<ul style="list-style-type: none"> If a website asks for information that is private, how do we deal with this appropriately Once we publish content it is easy to share and hard to remove e.g. video's and photographs Never meet anyone contacted through the internet. 	<ul style="list-style-type: none"> The internet can be very exciting but children need to follow rules to remain safe. To question the source of information. How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately. 	<ul style="list-style-type: none"> We should not fill out forms with a lot of personal details. Pupils learn what spam is, the forms it takes and identify strategies for dealing with it. 	<ul style="list-style-type: none"> Information put on line leaves a digital footprint or trail, this can be big or small, helpful or hurtful depending on how they manage it. Protect yourself from identity theft by how we share information 	<ul style="list-style-type: none"> Jigsaw Video

Curriculum Progression for teaching e-safety.

APPENDICES

APPENDIX 1	ICT Register of Access	11
APPENDIX 2	eSafety Information Leaflet	13
APPENDIX 3	Safety Rules for Children	15
APPENDIX 4	An Acceptable Use of the Internet	17
APPENDIX 5	Acceptable Use Agreements	20



ICT Register of Access – Clare Primary School

Access	Name	Role
SIMS System Manager (Access to entire SIMS system)	Miss Shona Lindsay Mrs Shirley Adair Mrs Anne Reid	Principal Secretary/Administrator ICT Co-Ordinator
C2k Manager	Mrs Anne Reid Mrs Shirley Adair Mrs Natalie Turkington	ICT Co-Ordinator Secretary/Administrator Numeracy/Assessment Co-Ordinator
SIMS Exams Officer (Post Primary Only)	N/A	
SIMS Attendance Manager	Miss Shona Lindsay Mrs Anne Reid Mrs Shirley Adair	Principal ICT Co-Ordinator Secretary/Administrator
SIMS Personnel Officer	Miss Shona Lindsay Mrs Anne Reid Mrs Shirley Adair	Principal ICT Co-Ordinator Secretary/Administrator
SIMS SEN Coordinator	Miss Shona Lindsay Mrs Anne Reid	Principal ICT Co-Ordinator
SIMS School Administrator	Mrs Shirley Adair	Secretary/Administrator
SIMS Pastoral Manager	Mrs Shirley Adair	Secretary/Administrator
SIMS Assessment Manager/Co-Ordinator	Miss Shona Lindsay Mrs Anne Reid Mrs Shirley Adair Mrs Natalie Turkington	Principal ICT Co-Ordinator Secretary/Administrator Assessment Co-Ordinator
FMS	Mrs Shirley Adair Miss Shona Lindsay	Secretary/Administrator Principal
Private Folder 1	Miss Shona Lindsay	Principal
Private Folder 2	Mrs Grace Martin Miss Shona Lindsay	Designated Child Protection Teacher Deputy Designated Child Protection Teacher
Private Folder 3	Miss Shona Lindsay	Principal
Private Folder 4	Mrs Shirley Adair Miss Shona Lindsay	Secretary/Administrator Principal
Private Folder 5	Miss Shona Lindsay	Principal

Access	Name	Role
Private Folder 6	Miss Shona Lindsay	Principal
Private Folder 7	Miss Shona Lindsay	Principal
Private Folder 8	Miss Shona Lindsay	Principal
Private Folder 9	Miss Shona Lindsay	Principal
Private Folder 10	Miss Shona Lindsay	Principal
Delegated Filtering Access (If school have opted in)	Mrs Anne Reid	ICT Co-Ordinator
Securus (If school have opted in)		
Staff Access to Pupil Folders (EN118)	Mrs Anne Reid Mrs Shirley Adair Mrs Natalie Turkington	ICT Co-Ordinator Secretary/Administrator Numeracy/Assessment Co-Ordinator
File & Folder Permission Tool (EN135)	Mrs Anne Reid Mrs Shirley Adair	ICT Co-Ordinator Secretary/Administrator
Text Messaging	Mrs Anne Reid	ICT Co-Ordinator

APPENDIX 2

Promoting e-Safety In the Home

- Keep computer/laptop/devices in a communal space
- Monitor time spent on-line, be aware that children may be using the Internet during the night when you think they are sleeping
- Monitor the websites visited
- Talk to children about how they are using the Internet/what they are doing
- Check your Internet filters - are parental controls necessary?
- Remind children never to give out personal information, share photographs of themselves or others online or meet up with people
- Do your research - find out about game content, social media filters/security etc
- Be mindful of what you as a parent/guardian post online especially on social media - you could be putting your child at risk!

It is important to talk to your children about e-safety so that they are aware of the potential risks and dangers they may face whilst using the Internet. The following: 'Things to consider...' offers a useful starting point.



Useful Websites and Sources of Additional Information



www.childnet.com



www.nspcc.org.uk



www.thinkuknow.co.uk



www.saferinternet.org.uk

www.bbc.co.uk/cbbc/findoutmore/stay-safe-useful-links



www.internetmatters.org

Clare Primary School



e-Safety Information Leaflet for Parents/Guardians



www.clareprimary.com

Revised: January 2019

What is ICT& how does this relate to e-Safety?

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 (e-Safety) associated with the use of Internet technologies.

e-Safety in School

In Clare Primary School we are committed to providing a safe and secure learning environment for all children. We understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them 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.



How is e-Safety encouraged in school?

- Pupils and Staff must agree to an 'Acceptable Use of the Internet' Agreement

- e-Safety will be delivered throughout the curriculum e.g. participation in Safer Internet Day
- e-Safety 'SMART' posters are displayed throughout the school
- Pupils are reminded about safe Internet use before and during lessons where appropriate
- 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
- The school Internet access is filtered through the C2k managed service.



What are my responsibilities as a Parent/Guardian?

As Parent's/Guardians there is a responsibility towards encouraging, educating and practising good eSafety (Internet/Online Safety) outside of school. School cannot be held responsible for matters which originate outside of school. At home parent's/guardians are responsible for monitoring Internet activity.

This leaflet aims to provide Parent's/Guardians with additional information surrounding eSafety and other sources of support to enable them to help keep their children safe.

What do I do if I have a concern/complaint about e-Safety?

Please inform the school immediately if you have a concern regarding e-Safety. The class teacher will work with the ICT Co-Ordinator (Mrs Reid) and Principal (Miss Lindsay) to address and resolve an issue or concerns. Should further action be required this will be addressed with the chairperson of the Board of Governors, Mr M. Adair.

School cannot be held responsible for cyberbullying (bullying which takes place over digital devices) matters that originate outside of school. However matters relating to Safeguarding or Pastoral Care will be addressed by Mrs Martin (Designated Teacher for Child Protection) and Miss Lindsay (Deputy Designated Teacher for Child Protection).



Cyberbullying - 10 things you need to know
www.internetmatters.org

1. Cyberbullying is growing - 20% of 13-18 yr olds claim to have been cyberbullied
2. The Internet never sleeps - It can happen anytime, anywhere
3. It's easy to do and get involved in
4. It can be anonymous
5. Talk about it - discuss social media and the associated risks before it's too late
6. Be aware what children are sharing online and appropriate content
7. Parental controls and Privacy settings can help protect against Cyberbullying
8. Explore for yourself - learn about the apps, social media and games your child is using
9. Take it seriously - check in with your child and be mindful of the signs of being bullied
10. Block and report - teach your child what to do if they want to prevent or report abusive messages.

APPENDIX 3

Safety Rules for Children

Follow These SMART TIPS

**S**

Safe - 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, IM messages 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**

Reliable - 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! Always check information by looking at other sources. Only chat on-line with people you know.

**T**

Tell your parent or carer if someone or something makes you feel uncomfortable or worried or if you or someone you know is being bullied on-line.

<h1>S</h1> <h2><u>S</u>tay <u>S</u>afe</h2> <p>Don't give out your personal information to people / places you don't know.</p> 	<h1>M</h1> <h2><u>D</u>on't <u>M</u>ee<u>t</u> Up</h2> <p>Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.</p> 	<h1>A</h1> <h2><u>A</u>ccepting <u>F</u>iles</h2> <p>Accepting emails, files, pictures or texts from people you don't know can cause problems.</p> 	<h1>R</h1> <h2><u>R</u>eliable?</h2> <p>Check information before you believe it. Is the person or website telling the truth?</p> 	<h1>T</h1> <h2><u>T</u>ell <u>S</u>omeone</h2> <p>Tell an adult if someone or something makes you feel worried or uncomfortable.</p> <div data-bbox="1646 1045 1937 1316"> <p>Follow these SMART tips to keep yourself safe online!</p> </div> <div data-bbox="1747 1332 1937 1388"> <p>© Teaching Ideas www.teachingideas.co.uk</p> </div>
---	--	---	---	---

SMART tips based on resources from www.thinkuknow.co.uk

APPENDIX 4

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 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/carers will be informed.

APPENDIX 4



Child's name: _____

Date: _____

Clare Primary School ICT Acceptable Use Agreement

ICT covers a wide range of resources and plays an important role in education today. Currently we have computers, iPads and Smartboards that are used daily in every classroom.

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

In Clare Primary School we understand the responsibility to educate our pupils in internet and e-Safety issues. We aim to teach them 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.

A copy of the school Internet policy will be available on the new school website when it is launched later this month for your reference if you require further information. In accordance with this policy, all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's internet and E-Safety rules.

Acceptable Use Agreement

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's name: _____

Date: _____

As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email if applicable. 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.

Signed: _____

Date: _____

Clare Primary School Photographic Permissions

As part of school life, opportunities arise for photographs of class activities and individual children to be displayed online or in the local press. In keeping with good practice relating to child protection, I wish to seek your permission for the use of these photographs.

☐ **I give permission for photographs of my child to be used in school**

These photographs are often displayed in school and parent, pupils, staff and visitors enjoy looking at the colourful wall display.

☐ **I give permission for photographs of my child to be used for publicity**

Sometimes photographs may be taken to be published in the school prospectus, brochures, newspapers or ELB publications e.g. competition/award winners.

☐ **I give permission for photographs of my child to be used on school website**

To celebrate the success of teams and individuals, photographs of groups/classes or individuals displaying work may be uploaded onto the school website. (Names of individual children will not be displayed beside photographs used).

☐ **I give permission for photographs of my child to be used on school social media pages**

Photos posted to Facebook or Twitter may be liked, shared or retweeted by other individuals and organisations beyond the control of the school, for example a tweet relating to a school trip to the Kingspan stadium may be retweeted by Ulster Rugby

N.B In line with our Child Protection Policy, no photographs of children will be used on websites of other organisations without additional parental consent.

Signed: _____

Date: _____

Clare Primary School**PE**

It is not compulsory for children to change for Curricular P.E. as suitable clothing is worn to school on the designated day(s). Primary 4 – Primary 7 children will be given the opportunity to change for Curricular P.E. and may do so unsupervised and in separate changing areas for girls / boys. All children who participate in an After School Activity will change, independently, unsupervised and in separate changing areas for girls / boys.

Signed: _____

Date: _____

Clare Primary School**School Trips**

I give permission for my child to attend all educational outings, trips to cinema, pantomime, etc., walks in and around the Clare area and all extracurricular activities. We understand that we will be informed of outings requiring buses etc. and if I/we have any objections to the child's attendance I will contact the school.

On occasion it may be necessary for your child/children to travel in an insured staff member's car, for example to transport sports teams to events, etc. If this is the case I provide permission for my child to travel in a staff member's car and will be required to provide a child/booster seat.

Signed: _____

Date: _____

APPENDIX 5

Clare Primary School Acceptable Use Agreement – 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

Clare Primary School Internet Streaming – Acceptable Use Agreement



Overview

The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What's Different?

Previously, primary schools had no school control over the internet sites available, and postprimary and special schools had access to a number of internet "amber groups" to which users could be added. The new system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:

In addition to the default sites, schools can choose to make users members of one or more internet-related security groups. These are:

- Internet Social Networking
- Internet Streaming Media
- Internet Advanced

Access to these groups is controlled by the C2k Manager who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL.

Internet Streaming

This group provides access to YouTube, BBC iPlayer, Vimeo and other television and radio streaming sites. When a user is added to the Internet Streaming security group the following categories, RED in the Default policy, are now GREEN.

Clare Primary School Implications

If a member of staff is to be added to the Internet Streaming groups they must agree to the following:

- To check all video that is to be shown to classes before use
- Be responsible for the content of any video shown to a class
- To use in an appropriate manner and in accordance with the guidelines detailed in the school's E-Safety Policy and Child Protection Policy

I agree to the terms of the Internet Streaming Acceptable Use Agreement and wish to be added to this group.

Signed _____

Date _____

Clare Primary School

Advanced Internet Streaming – Acceptable Use Agreement



Overview

The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What's Different?

Previously, primary schools had no school control over the internet sites available, and postprimary and special schools had access to a number of internet "amber groups" to which users could be added. The new system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:

In addition to the default sites, schools can choose to make users members of one or more internet-related security groups. These are:

- Internet Social Networking
- Internet Streaming Media
- Internet Advanced

Access to these groups is controlled by the C2k Manager who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL.

Internet Advanced

This group provides access to a range of websites that contain adult material. These include: webmail, shopping, drugs and alcohol, sex education. When a user is added to the Internet Advanced security group these categories, RED in the Default policy, are now GREEN. A full list of categories can be found on information sheet E039

Clare Primary School Implications

If a member of staff is to be added to the Internet Advanced groups they must agree to the following:

- To check all websites before they are shown to classes
- Be responsible for the content of any websites shown to a class
- To use in an appropriate manner and in accordance with the guidelines detailed in the school's E-Safety Policy and Child Protection Policy

I agree to the terms of the Internet Advanced Acceptable Use Agreement and wish to be added to this group.

Signed _____

Date _____