



Creggan Primary School /
'Learning for Life'

Creggan Primary School

Online Safety Policy

Reviewed: September 25

Review date: September 28

Sean McAuley	
Chair of Board of Governors	Date
Karen McElroy	
Principal	Date

In Creggan Primary we believe that e-safety is an essential element of safeguarding children and adults in the digital world when using technology. We recognise that the internet and information communication technologies are now an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online. In Creggan Primary School, we believe it is our duty to provide the school community with quality internet access to raise educational standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. We identify a clear duty to ensure that children are protected from potential harm online and develop the skills and knowledge necessary to stay safe online. It is our responsibility to ensure there is a reduced risk of pupils accessing harmful and inappropriate digital content and should support and empower pupils to engage in online activities in an educated, safe, responsible and respectful way.

Online safety means acting and staying safe when using digital technologies. It is wider than simply internet technology and includes electronic communication messages, social environments and apps, and using games consoles through any digital device.

In January 2014, the SBNI published its report 'An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland' which identified the associated risks around online safety under four categories below:

- **Content risks:** The child or young person is exposed to harmful material
- **Contact risks:** The child or young person participates in adult initiated online activity
- **Conduct risks:** The child or young person is a perpetrator or victim in peer-to-peer exchange
- **Commercial risks:** The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs

What is ICT?

The term, Information and Communications Technology (ICT) covers a range of resources from traditional computer-based technologies to the fast evolving digital communication technologies.

Some of the Internet-based and electronic communications technologies which children are using, both inside and outside of the classroom, are:

- Websites
- Learning Platforms / Virtual Learning Environments
- Email and Instant Messaging
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- iPads and other tablet devices with internet access

While 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 their use.

What is Online Safety?

Online Safety encompasses internet technologies and electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- Online Safety concerns safeguarding staff, children and young people in the digital world.
- Online Safety emphasises learning to understand and use new technologies in a positive way.
- Online Safety is less about restriction and more on education about the risks as well as the benefits so pupils and staff can feel confident online.
- Online Safety is concerned with supporting staff, children and young people to develop safer online behaviours both in and out of school.

In Creggan Primary School we understand our responsibility to educate pupils in Online Safety. We aim to teach children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

A Consistent Whole School Approach

- All teaching and non-teaching staff in Creggan Primary can recognise and are aware of online safety risks.
- Online safety messages are integrated across the curriculum for pupils in all Key Stages.
- Online safety messages are distributed amongst pupils, staff, parents/carers and the wider community.
- The school's leadership and management have clearly prioritised online safety and safeguarding across all areas of the school.
- Knowledge is shared amongst staff and there are good capacity-building opportunities.

Risks and Responses

The Internet is an 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

In our school children will 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

- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information (e.g. send inappropriate photographs) 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.

In our school 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.

Cyber Bullying

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites. If it takes place within school, cyberbullying will be dealt with in line with the school's overall Addressing-Bullying policy, Positive Behaviour Policy and Safeguarding/Child Protection Policy.

In our school children will be taught:

- If they feel they are being bullied through social networking sites, text or online they should always tell someone they trust.
- Not to reply to bullying, threatening messages as this could make things worse.
- Not to send or forward abusive messages or images to anyone.
- Keep abusive messages as evidence.

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Online Safety Week is celebrated in Creggan PS each term with Internet Safety Day in February. During these weeks lessons will focus on staying safe online, assemblies to reinforce safety messages and children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school.

Roles and Responsibilities

As Online 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/ Designated Teacher for Child Protection (Mrs Joan Martin) to keep abreast of current Online Safety

issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) the Safer Schools App and Childnet. Mrs Martin and Our Principal, Mrs McElroy, have responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal (Mrs McElroy) and ICT Co-ordinator (Mrs J Martin) will update Staff 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.

Management of Personal Data

- Creggan Primary has effective policies and procedures in place which ensure personal data is collected and managed responsibly
- All communications between the school and pupils, their families/carers and external agencies delivered using technology should be clear and professional.
- The school has a clear process for transferring data to third parties. (DE Circular 2015/13)

Writing and Reviewing the Online Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the Principal, Staff and approved by the Governing Body.

The Online Safety Policy and its implementation will be reviewed annually.

Development for Staff

- All staff receive regular information and training on Online Safety issues through the co-ordinator at staff meetings or Staff Development Days.
- 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 Online Safety Policy and Acceptable Use Agreement as part of their induction.
- All teachers are encouraged to incorporate Online-Safety activities and awareness within their lessons.

Online Safety Information for Parents/Carers

Parents/carers have an important role to play in promoting Online Safety. We encourage all parents/carers to become involved in Online Safety discussions and activities with their child.

- The school communicates relevant Online Safety information through parents' monthly Sway Newsletters and weekly class See Saw Messages.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement/Code of Conduct with their child.
- Parents/carers are required to give written consent to images of their child being taken/used on the school website.
- Parents are encouraged to sign up to the Safer Schools App

During Internet Safety Week, parents will be reminded that it is important to promote Online Safety in the home and to monitor Internet use. The following guidelines are provided:

- 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 and the "Click Clever, Click Safe" code
- 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.
- Useful website links are used both in school and provided to parents for use at home:
 - www.childnet.com
 - cbbc/topics/stay-safe
 - www.thinkuknow.co.uk/
 - www.saferinternet.org.uk
 - www.commonsense.org

Teaching and Learning

In Creggan Primary, we have clear progression from P1-P7 for teaching and learning of Online Safety.

- Teachers will plan for and provide opportunities across the curriculum for children to develop their e-Safety skills.
- Key Stage 1 and 2 Pupils will follow the CCEA Internet Safety programmes:
<https://ccea.org.uk/learning-resources/digital-life-and-work> **Foundation -Key Stage 2**
<https://ccea.org.uk/document/15009> **Key Stage 2**
<https://ccea.org.uk/learning-resources/scamwise>
<https://www.commonsense.org/education>
- Educating children on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise, and as part of the e-Safety and preventative curriculum using the NSPCC PANTS Programme and the Barnados Paths Programme.
- Children are made aware of the impact of online bullying and know how to seek help if these issues affect them. Children are also made 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 using a Websense filtering solution.
- 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.
- Children are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Children are 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.
- 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. They will be taught to be "Click Clever, Click Safe":

Zip it (never give personal data over the internet)

Block it (block people you don't know)

Flag it (if you see something you don't like flag it up with someone you trust).

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.
- Sending or displaying insulting or offensive messages/pictures is forbidden.
- Using obscene language is forbidden

Social Networking:

- Through the C2k system our school currently blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- 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 – See Code of Conduct

Portable Technologies:

- The use of portable devices 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. All staff use One drive to store data on.
- Pupils are not allowed to bring personal mobile phones to school.
- 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/ Facebook Page. 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.
- 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/Code of Conduct 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/guardians will be asked to sign the Acceptable Use Agreement/Code of Conduct for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Staff Code of Conduct before using any school ICT resource.

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. They are encouraged to keep details of usernames and passwords private.
- 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 Online Safety Complaints:

- Complaints of Internet misuse will be dealt with by The Principal, Mrs K McElroy, and the ICT Co-Ordinator (Mrs J Martin).
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator.
- As part of the Acceptable Use Agreement children will know that if they deliberately break the rules they could be stopped from using the Internet/E-mail and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.(Designated Teacher for Child Protection, Mrs Martin, in her absence, Mrs McElroy)
- Complaints regarding cyberbullying will be dealt with in line with the school Addressing Bullying Policy.
- Pupils and parents will be informed of the complaints' procedure.
- Any complaint about staff misuse must be referred to the Principal and governors.

Communicating the Policy:

Introducing the Online Safety Policy to pupils

- Online 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/ Paths Programme and NSPCC Keeping Safe Programme.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the Online Safety Policy:

- All staff will be involved in discussions regarding Online Safety and will have a copy of this Policy.
- Staff will be aware that Internet use can be monitored and traced to the individual. 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.
- Staff are advised not to use their own personal phones or devices for taking photographs or contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone where contact with pupils or parents is required

Staff should follow the guidelines below:

- Never communicate with pupils outside of school via social networking sites and chat rooms.
- Never respond to informal, social texts from pupils
- Never use personal technology to take images or videos of children

Monitoring and review:

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

This policy is the governors' responsibility and they will review its effectiveness annually. They will do this through liaison with the ICT Co-ordinator and the Designated Child Protection Teacher – Joan Martin

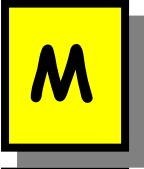
Safety Rules for Children

Follow These SMART TIPS



S

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



M

Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



A

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



R

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



T

Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committee

Dear Parents

Children should know that they are responsible for making an Acceptable Use of the Internet. We would ask you to discuss these rules for Acceptable Use of the Internet with your child. We would ask if you could sign the acceptable use agreement overleaf, with your child.

- 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 or App, 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/online messages 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 collaborating online 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 trusted adult immediately.
- I will not bring in memory sticks or mobile devices 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/ online messages 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.

An Acceptable Use of the Internet

P2-P4

Dear Parents

Children should know that they are responsible for making an Acceptable Use of the Internet. We would ask you to discuss these rules for Acceptable Use of the Internet with your child. We would ask if you could sign the acceptable use agreement overleaf with your child.

- I will only use my own login username and password when logging in to school computers
- I will keep my username and password private.
- I will not look at other people's files without their permission
- I will not change or delete other people's work.
- I will ask permission before entering any website, unless my teacher has already approved

CREGGAN PRIMARY SCHOOL**Acceptable Use Agreement
For Pupils**

Please discuss the Acceptable Use rules with your child and then 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	

Parent's Name			
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 daughter or son to follow when selecting, sharing and exploring information.			
Parent's Name (print)			
Parent's Signature		Date	

CREGGAN 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 e-Safety Policy has been drawn up to protect all parties – the children, 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.

- Internet use should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised C2K account and password, which should not be made available to any other person
- The C2k email account should be used for professional purposes.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mail being received
- 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 or send inappropriate materials such as pornographic, racist or offensive material is forbidden
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- "My Documents" is property of the school and the school Principal can access this at any time
- Social networking is prohibited within school. Personal use outside of school hours should not involve any communication regarding school business.
- Mobile phones should only be used when necessary – to receive phone calls from GP/hospital/family member or emergency purposes.

Name:

Date:

Signed:

An Acceptable Use of the Internet

P1

Dear Parents

Children should know that they are responsible for making an Acceptable Use of the Internet. We would ask you to discuss these rules for Acceptable Use of the Internet with your child. We would ask if you could sign the acceptable use agreement overleaf with your child.

- The Classroom assistant or my teacher will log me in to the computer using a pupil username and password.
- I will not look at other people's files without their permission
- I will not change or delete other people's work/files.
- I will ask permission before using websites or Apps, unless my teacher has already approved that site.