Macosquin Primary School

E-SAFETY POLICY

(Previously known as 'Safe and Effective Use Policy for the Internet and Digital Technologies')

CONTEXT

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circulars 2011/22, 2013/25 and 2016/27 on e-Safety. This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Macosquin Primary School. It also links to Article 17 from the UN Convention on the Rights of the Child which states:

"You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure the information you are getting is not harmful, and help you find and understand the information you need."

WHAT IS e-SAFETY?

e-Safety is short for electronic safety.

This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology as well as collaboration tools and personal publishing.

e-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources; including online assessment:
- rapid and cost effective communication;
- gaining an understanding of people and cultures around the globe;
- staff professional development through access to new curriculum materials, shared knowledge and practice;
- greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others;
- social and leisure use.

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.

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. This e-Safety policy reflects this by keeping abreast of the changes taking place. In our School we have a duty of care to enable pupils to use on-line systems safely.

This e-Safety policy operates in conjunction with other school policies including Positive Behaviour, Child Protection/Safeguarding Children, Anti-Bullying, Mobile Phones and other Related Technologies. E-Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the Northern Ireland curriculum and schools must ensure acquisition and development by pupils of these skills.

This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety in Macosquin Primary School depends on effective practice at a number of levels:

 responsible ICT use by all staff and students; encouraged by education and made explicit through published policies;

 sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use;

 safe and secure internet provision by C2K and Classnet (maintained by specialised IT Technician).

CARE AND RESPONSIBILITY

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe internet access at all times. With these opportunities we also have to recognise the risks associated with the internet and related technologies.

The use of these exciting and innovative tools in schools and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers pupils may face include:

 access to illegal, harmful or inappropriate images or other content;

 unauthorised access to/loss of/sharing of personal information;

 the risk of being subject to grooming by those with whom they make contact on the Internet;

 the sharing/distribution of personal images without an individual's consent or knowledge;

 inappropriate communication/contact with others, including strangers;

 cyber-bullying;

 access to unsuitable video/internet games/materials;

 an inability to evaluate the quality, accuracy and relevance of information on the Internet;

 plagiarism and copyright infringement;

 illegal downloading of music or video files;

 the potential for excessive use which may impact on the social and emotional development and learning of the young person.

It is impossible to eliminate the risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise.

PREVENTATIVE

In Macosquin Primary School we understand the responsibility to educate our pupils in e-Safety issues. Our School builds a preventative curriculum; we aim to teach pupils to behave appropriately and think critically enabling them to remain both safe and within the law when using the Internet and related technologies, in and beyond the context of the classroom

 The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety. We will use specific digital lessons to cover the different curriculum areas throughout the year which will be age and content appropriate for each year group (Refer to e-safety scheme folder in Principal's Office).

 Educating pupils on the dangers of technologies that may be encountered outside of school will be discussed with pupils in an age appropriate way on a regular basis by teachers and other agencies (as appropriate – E.g. PSNI as part of the CASE programme).

 Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of how to seek advice or help if they experience problems when online. E.g. from a parent/ carers, teacher/ trusted member of staff.

 The school internet access is filtered through the C2K managed service and Classnet;

 ICT Co-ordinator has set restrictions on all class ipads so children cannot install, download or purchase apps or have access to Safari. A restriction password is always required to change any of these restrictions for Safari or the app store.

 Use of the internet is a planned activity. Aimless surfing is prohibited. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class. Teachers will use the website restrictions to add specific websites relating to lessons on each ipad. This will enable children to safely access internet pages during lessons.

 Pupils will be taught to use the internet as an aid to learning.

 The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

 Children will be taught to be **'Internet Wise'** and therefore good online citizens and are encouraged to discuss how to cope if they come across inappropriate content. Posters will be displayed in every classroom to encourage this. (Refer to Appendix 5 – a sample is included here.)

 All teachers will teach two e-safety lessons each half term from the e-safety scheme. Internet Safety Week will be planned for by teaching staff through key stage assemblies, lessons and a homework activity.

 Children will know which staff members to go to for help by looking at the 'We are Here to Help' display board. In Macosquin Primary School we promote a positive, caring ethos where our children feel valued and listened to at all times. Worry boxes will be displayed in classrooms and PDMU/Circle Time activities planned for accordingly.
 Parent training will be provided to provide information on how to keep their child safe on the internet at home. Parents will be informed about the Vodaphone website on digital parenting.
https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/child_safety_online.html#cso1

ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of Child Protection/Safeguarding Children within the school therefore, the school's e-Safety Team, 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 e-Safety co-ordinator and the e-Safety Team including 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. This team has the responsibility for leading and monitoring the implementation of e-Safety throughout the school.

The e-Safety co-ordinator/Principal have the responsibility to update Senior Leadership Team and Governors with regard to e-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

e-Safety Responsibilities: e-Safety Co-ordinator

Our e-Safety coordinator is the person responsible to the Principal and the Board of Governors for the day-to-day issues relating to e-Safety.

The e-Safety co-ordinator:

 leads the e-Safety team as well as discussions on e-Safety with the School Council;

 takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents;

 ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident;

 provides training and advice for staff;

 liaises with the Education Authority;

 receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments;

 reports regularly to Senior Leadership Team;

 receives appropriate training and support to fulfil his/her role effectively;

 has responsibility for blocking/unblocking internet sites on C2K and Classnet;

 passing on requests for blocking/unblocking to the C2K helpdesk and/or Classnet;

 maintains the e-Safety Log Book indicating any occasions where the school has used its powers of search and deletion of material on electronic devices (E.g. inappropriate photographs).

e-Safety Responsibilities - The Board of Governors:

 are responsible for the approval of this policy and for reviewing its effectiveness. The Governors should receive regular information about e-Safety incidents and monitoring reports.

 Monitor and track outcomes through Safeguarding Team Meetings.

 Receive appropriate training to support the Principal and Leadership team.

e-safety Responsibilities - The Leadership Team:

 is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day-to-day responsibility for e-Safety is delegated to the e-Safety co-ordinator;

 and Head of Pastoral Care and Child Protection should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member

of staff. Refer to staff disciplinary procedures, and/or Child Protection/Safeguarding Children Policy.

e-Safety Responsibilities - Teaching and Support Staff must:

 have an up-to-date awareness of e-Safety matters and of the current school e-Safety policy and practices;

 embed e-Safety issues into the curriculum and other school activities as appropriate;

 have read, understood and signed the school's Acceptable Use of the Internet Policy for staff/volunteer for ICT/ipads (see Appendix 1);

 report any suspected misuse or problem to the school's e-Safety co-ordinator.

e-Safety Responsibilities for Pupils

Pupils need to know how to cope if they come across inappropriate material or situations online. e-Safety will be discussed with pupils on an ongoing and regular basis. This should be discussed with the pupils in an age-appropriate way as a set of rules that will keep everyone safe when using technology in school. (Refer to Appendix 2 and Appendix 2a.) It will also be discussed as they accept the agreement through their MySchool log in.

Activities throughout the school year including Safer Internet Day and visits from the PSNI will reinforce e-Safety and further pupils' understanding.

Teachers will deliver a series of appropriate and progressive lessons on e-safety throughout the year focusing primarily on raising awareness of the associated risks around online safety and promoting to children ways in which to deal with these. The risks have been defined under four categories:

- Content risks – The child or young person is exposed to harmful materials.
- Contact risks – The child or young person participates in adult-initiated online activity and/or is at risk of grooming.
- Conduct risks – The child or young person is a perpetrator or subject to behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.
- Commercial risks – The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

There are clearly defined procedures for reporting and dealing with incidents surrounding breaches in the school's online safety guidelines and children are aware of how to report an issue or concern.

Refer to Appendix 3: Resources

Refer to Appendix 3a: How to report an incident

e-Safety Responsibilities for Staff

All staff will be introduced to the e-Safety Policy and its importance explained. Staff will be asked to read and sign the Acceptable Use of the Internet Agreement for Staff (Refer to Appendix 1) which focuses on e-safety responsibilities in accordance with the Staff Code of Conduct. Staff should be aware that all Internet traffic (including email) is monitored, recorded and tracked by the C2K and Classnet systems.

Photographs/stills or video footage of pupils should only be taken using school equipment for purposes authorised by the School. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be retained and destroyed in accordance with the schools Records Management Policy and Disposal Schedules.

Staff have access to Youtube (for educational purposes only) when logged into C2K system. Therefore staff must ensure that no pupil is given access to a computer that they are logged on to unless being supervised.

Staff should always ensure that any Internet searches involving sites that have been granted enhanced access to should **not** be carried out when children can view them, i.e. on the computer's screen or on an interactive whiteboard. Youtube should only be used after the content has been viewed and checked, ensuring that children are not exposed to inappropriate content.

e-Safety responsibilities for Parents

Macosquin Primary School will look to promote e-Safety awareness within the school community which may take the form of information evenings for parents/carers, information leaflets and/or links on the school website. Parents will be encouraged to work in partnership with the School and support their child in all aspects of e-Safety. They should advise their child to report any e-safety issues to their class teacher or designated adult in School ('We are Here to Help' display and e-Safety Posters around the school).

Information for parents is available on the following websites:

www.thinkyouknow.co.uk A mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
www.bbc.co.uk/webwise Includes and 'Internet for Beginners' course and a tool for answering your internet related questions.
www.kidsmart.org.uk Explains the SMART rules for safe internet use and lots more besides.
www.ceop.gov.uk The Government's Child Exploitation and Online Protection Centre (CEOP).
www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use.

e-SAFETY SKILLS DEVELOPMENT FOR STAFF

e-Safety training is an essential element of staff induction and should be part of on-going Continuous Professional Development programme. Through this e-Safety policy, we aim to ensure that all reasonable actions are taken and measures put in place to protect all users.

 All staff will receive regular information and yearly training on e-Safety issues through the e-Safety co-ordinator /ICT co-ordinator at staff meetings/ Baker Days.

 All staff must be 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.

 All staff are encouraged to incorporate two e-Safety lessons per half term into their planners and promote awareness within their lessons.

 All staff members will receive a copy of this e-Safety policy and Acceptable Use of the Internet Agreement. All staff should read and sign the Acceptable Use of the Internet Agreement (Refer to Appendix 1).

HANDLING OF e-SAFETY

To deal with any incidents of technology misuse by pupils which arise, the school's Positive Behaviour Policy will be followed. Pupils must be made aware the repeated misuse of the Internet may lead to their access to it being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.
Where the incident involves child abuse, the Designated Teacher for Child Protection/Safeguarding Children in the school must be notified and the school will follow procedures as set out in the school's Child Protection/Safeguarding Children Policy.

Issues of Internet misuse and access to any inappropriate material by any user should be reported immediately to the school's e-Safety Co-ordinator and recorded in the school's e-Safety log, giving details of the site and the time.

A record of very serious incidents will be kept in the locked Child Protection/Safeguarding Children cabinet within school.

Harassment of another person using technology, or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences.

For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed and advice will be sought from the P.S.N.I.

After a minor or major incident a comprehensive debriefing will occur to review school policy and procedures.

Logs of misuse, changes to filtering controls and of filtering incidents are made available to the:

- Senior Leadership Team;
- Principal;
- Board of Governors;
- e-Safety Team.

If police involvement is necessary, the Principal/e-Safety Co-ordinator/Board of Governors will seek advice from Schools' Branch and the legal department at the Education Authority.

e-SAFETY TEAM

The school's e-Safety team consists of:

▪ Mrs Louanne McElwee	Principal, DDT for Child Protection/ Safeguarding and C2K Manager
▪ Mrs Cathy Allen	ICT and e-safety Co-ordinator, C2K Manager, Designated Teacher for Child Protection/ Safeguarding / Pastoral Care
▪ Mr Paul Grant	DDT for Child Protection/ Safeguarding/ C2K Manager
▪ Mr Edward Jamison	Designated Safeguarding Governor

ILLEGAL or INAPPROPRIATE ACTIVITIES

The school believes that the activities listed below are inappropriate (and on occasions illegal) in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school). Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Regard should be given to the School's e-safety policy at all times both inside and outside of work. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

 child sexual abuse images (illegal - The Protection of Children Act 1978); grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003);

 possession of pornographic images (illegal – Criminal Justice and Immigration Act 2008 criminally racist material in UK – to stir up religious hatred or hatred on the grounds of sexual orientation) (Illegal – Public Order Act 1986);

 promotion of any kind of discrimination;

 promotion of racial or religious hatred;

 threatening behaviour, including promotion of physical violence or mental harm;

 any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally, the following activities are also considered unacceptable on school ICT equipment provided by the school:

 using school systems to run a private business;

 use systems, applications, websites or other mechanisms that bypass the filtering or

other safeguards employed by C2K and/or Classnet;

 uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;

 revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords);

 creating or propagating computer viruses or other harmful files;

 on-line gambling and non-educational gaming;

 use of personal social networking sites/profiles for non-educational purposes. Staff and volunteers should ensure that they adopt suitably high security settings on any personal profiles they may have.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. (Refer to Appendix 4)

INTERNET SECURITY – C2K

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution.

Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school Principal.

Connection of non C2K devices to the Internet e.g. iPads can be connected through the controlled C2K guest wireless network and is subject to the same level of filtering as the main school system.

INTERNET SECURITY – CLASSNET

Due to poor infrastructure within specific areas of the school, we also use a second internet system 'Classnet'. Classnet is maintained with an active, monitored filter system to satisfy both the needs of child protection/ inappropriate content whilst ensuring that it serves to support teaching and learning.

This system exists in parallel to all C2K infrastructure. In line with DENI requirements the school has ensured that this additional service is:

a) filtered to standardised child protection levels;

b) supported by trained staff in its use.

Access to the Classnet network is governed by unique device registration and pre-approval by authorised staff only (ICT co-ordinator, SLT and Principal). No devices can join the network without this approval and authentication.

Only the following devices will be granted access to Classnet:

 school owned iPads;

Staff are not permitted to use mobile phones on the Classnet network.

The school will take appropriate measures to safeguard non-C2K equipment against security breaches.

Restrictions on Classnet:

The ICT Co-ordinator has set strict restrictions on all class ipads which prohibits children from accessing websites through Safari. The standard browser of Safari has been removed off all ipads. This can only be made assessible if the class teachers allows supervised access to specific websites, all controlled securely through the website restrictions.

Restrictions have also been set on the installing, deleting and purchasing of apps from the app store. Only Teaching Staff can install or delete apps. Any apps wishing to be purchased must be cleared first by the Principal and ICT Co-ordinator.

RISK ASSESSMENTS

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks.

The school has performed a risk assessment on the technologies within the school to ensure that they are fully aware of and can limit the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or

situations online. The school risk assessment will inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.

Refer to Appendix 6: Risk Assessment

E-MAIL USE

 C2k recommends that all staff and pupils should be encouraged to use their C2k email system for school business. It is strongly advised that staff should not use personal email accounts for school business.

 The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

 Pupils must immediately tell a teacher when using their C2K email address (if activated) if they receive an 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 by staff or pupils is not permitted.

 Children will not always be given individual C2K e-mail addresses. In some instances, children may have access to a group e-mail to communicate with other children as part of a particular project. Messages sent and received in this way will be supervised by the teacher.

SCHOOL WEBSITE

Macosquin Primary School's website promotes and provides up-to-date information about the school and showcases other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

 Group photos are used where possible, with general labels/captions;

 Only photographs of children with parental/carer consent will appear on the school's website.

 First names will be included with photographs on the website only if parent/carer permission has been given;

 The website does not include home addresses, telephone numbers, personal e-mail or any other personal information about pupils or staff.

 The point of contact to the school i.e. school telephone number, school address and email address.

SOCIAL NETWORKING

Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals).

Social environments enable any community to share resources and ideas amongst users. There are many excellent public examples of social software being used to support formal and informal educational practice amongst young people and amongst educators. They are also popular ways of enabling users to publish and share information, including photographs, video from webcams, video files and blogs about themselves and their interests.

C2k filters out services which are misused and block attempts to circumvent the filters. Pupils will not be allowed to use any social software which has not been approved by teaching staff and the C2K filtering service.

Staff and pupils are advised that it is not acceptable or school policy for them to be friends on social network sites (e.g. Facebook). Pupils in this school are told they should not request to be friends with a member of staff on a social network site. Equally, staff are also told that they must not request to be friends or accept requests to be friends with pupils or past pupils of the school on any such site. This is good practice in line with child protection/safeguarding children policy.

 The school C2K/Classnet systems deny access to social networking sites.

 Pupils and their parents/carers are 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.

 Cyber-bullying is addressed within this policy and staff are made aware that pupils may be subject to cyber-bullying via electronic methods of communication both in and out of school. (More information provided below).

 Our pupils are asked to report any incidents of cyber bullying to the school (Refer to Appendix 3a).

School networking through the use of Internet-based and other electronic social media tools is integrated into everyday life. Use of Facebook, Twitter, blogging, wikis and other online social media vehicles are now commonplace with the result that the lines

between work and personal life can become blurred. To protect staff, pupils and the reputation of the school the following guidelines should be followed:

 Staff **should not use school systems** to engage in **personal** social media activities, i.e. Facebook, Twitter, blogging, wikis etc. This inappropriate use of social media sites may be treated as a disciplinary matter;

 If staff use social media sites for personal use, they are reminded that they have a responsibility to ensure they are posting comments or images that are not detrimental to their position as a staff member of Macosquin Primary School, the privacy or rights of pupils or the reputation of the school. Images may include photographs from staff parties that could be misinterpreted and present the staff or the school, in a negative light. **A common sense approach to the use of social media websites is recommended.**

PASSWORD SECURITY

 Staff 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 and should be changed if it appears pupils have worked out an adult's password.

 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 Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

MOBILE PHONES AND OTHER RELATED TECHNOLOGIES

It is important to be aware of the safety issues regarding mobile phones and other devices which now increasingly have Internet access. For this reason, Macosquin Primary School has a specific policy on the acceptable use of mobile phones and related technologies.

Pupils are not allowed mobile phones or devices in school. In exceptional circumstances and in agreement with the class teacher and parent, a mobile will be kept in a locked drawer and switched off until 3pm.

Staff members should refrain from using their mobile phones or similar technology when in contact with children unless prior permission has been given by the Principal.

Staff members will only use school devices linked to C2K to store and access all information.

CYBER BULLYING

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. Pupils engaging in cyber bullying may be dealt with in line with the school's 'Positive Behaviour Policy' and 'Anti-Bullying Policy'.

Cyber Bullying can take many different forms and guises including:

 Email – nasty or abusive emails which may include viruses or inappropriate content;

 Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity;

 Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile;

 Online Gaming – abuse or harassment of someone using online multi-player gaming sites;

 Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people;

 Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
  http://www.legislation.gov.uk/nisi/1997/1180

- Malicious Communications (NI) Order 1988
  http://www.legislation.gov.uk/nisi/1988/1849

- The Communications Act 2003
  http://www.legislation.gov.uk/ukpga/2003/21

Pupils will be encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Macosquin Primary School will also keep good records of cyber-bullying incidents as outlined in the Anti-bullying Policy, to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions. These will be stored in a locked cabinet with the e-safety co-ordinator.

NETWORK ACCESS

Pupil access to the Internet is through a filtered service provided by C2K and/or Classnet, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse. Full restrictions are in place for non-C2K devices (ipads) in school.

If a member of staff is suspected of using any device with non C2K internet access (e.g. phones with 3G/4G capabilities) to access what is considered as illegal/inappropriate material (see above) disciplinary procedures may be followed.

Pupils must not use any personal electronic devices within school to access the internet or any messaging services.

ACCEPTABLE INTERNET USE POLICY FOR STAFF

The C2K 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 students, the staff and the school.

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

Staff should read and sign a copy of the school's Acceptable Internet Use Agreement for Staff and return it to the Principal. (Refer to Appendix 1)

POLICY REVIEW

This e-Safety policy implementation outcomes are monitored and tracked continually by staff and Governors ensuring successful impact. The policy is reviewed annually, to take into account new emerging technology, or if any outcomes gives cause for immediate review.

RELATED POLICIES

- Positive Behaviour
- Anti-Bullying
- Child Protection/Safeguarding Children and COVID-19 Addendum to this policy
- Mobile Phone
- Pastoral Care
- PDMU
- Health and Safety
- Staff Code of Conduct
- Social Media
- Remote Learning Policy
- Records Management Policy and Disposal Schedules

Policy Links / Legislation

- Safeguarding and Child Protection in Schools - A Guide for Schools, DENI, April 2017
- Pastoral Care in Schools: Promoting Positive Behaviour (2001)
- Children (NI) Order (1995)
- The Education (NI) Order (1998) - Articles 3&4
- Human Rights Act (1998) - came into force in NI in 2000
- DE Circular Welfare and Protection of Pupils - 2003/13
- On-line safety Circulars (2016/17), (2016/26) and (2016/27)

https://www.macosquinps.co.uk/cmsfiles/items/downloads/MacosquinPrimarySchoolChildProtectionPolicyCovid19Addendum-1.pdf

Useful Websites and Telephone Numbers

D.E.N.I. www.deni.gov.uk
N.I.A.B.F. www.niabf.org.uk
www.thinkyouknow.org
www.commonsensemedia.org
www.graphite.org (Digital Citizenship)

Childline NI 08001111
NSPCC (fullstop Campaign) 0808 800 5000