St Colmcille's High School

Online Safety Policy

Schedule for Developing, Monitoring and Reviewing Policy

Approval by the Board of Governors:

The implementation of this Online Safety policy will be monitored by:

Monitoring and reviewing: Annually in June, and only if required following a breach of safety.

The Board of Governors will receive regular reports on Online Safety including anonymous details of Online Safety incidents: This will be in conjunction with the Child Protection Report given to the Board of Governors.

Should serious Online Safety incidents take place, the following external persons or agencies should be informed: PSNI, Chair of BoG and EA

Table of Contents

1. Rationale

"*The school's actions on and governance of online safety must be reflected clearly within the school's safeguarding arrangements and Online Safety Policy. Safeguarding and promoting pupils' welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities*."

DENI Online Safety Guidance, Circular number 2016/27

It is the responsibility of the schools, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Online Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The School must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of the Policy

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of the School. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure Online Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to Online Safety incidents that occur outside of school hours, the School will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. Online Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of Online Safety incidents outside of the School, will be dealt with in accordance with School Policies.

3. Risk Assessment

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 — to become "Internet-wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against 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 assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.
DENI Online Safety Guidance, Circular number 2013/25

The main areas of risk for the School can be categorised as the Content, Contract and Conduct of activity.

1. **Content**
   - Access to illegal, harmful or inappropriate images or other content.
   - Access to unsuitable video / internet games.
   - An inability to evaluate the quality, accuracy and relevance of information on the Internet.

2. **Contact**
   - Inappropriate communication / contact with others, including strangers.
   - The risk of being subject to grooming by those whom they may make contract on the Internet.
   - Cyber-bullying.
   - Unauthorised access to / loss of / sharing of personal information.

3. **Conduct**
   - The potential for excessive use which may impact on the social and emotional development and learning of the young person.
   - Plagiarism and copyright infringement
   - Illegal downloading of music or video files
   - The sharing / distribution of personal images without an individual's consent or knowledge.

Many of these risks reflect situations in the offline world and it is essential that this Online Safety policy is used in conjunction with other School policies e.g. Positive Behaviour, Child Protection, Anti-Bullying and Acceptable Use, Mobile devices, Disposal of documents.
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

4. Roles and Responsibilities

4.1 Online Safety Team Leader

The Online Safety Team Leader will lead the Online Safety Team and takes day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

The Online Safety Leader will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provide training and advice for staff
- Liaise with C2K and school ICT technical staff
- Liaise with the EA and DENI on Online Safety developments
- Liaise with the technical staff
- Receive reports of Online Safety incidents and create a log of incidents to inform future Online Safety developments
- Meet regularly with VP of pastoral care to investigate abuse of social network sites by pupils
- attend relevant meetings with Board of Governors
- discuss current issues, review incident logs
- monitors and reports to senior staff through one of the Vice Principals any risks to staff of which the Online Safety coordinator is aware

4.2 Online Safety Officers / Designated Child Protection Officer / Designated Deputy Child Protection Officer

The Child Protection Officer (F Roche) and their deputy (F Hanna) will be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

4.3 Online Safety Committee

The Online Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring of the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governors.

Committee Members:

- School Principal : Mr S. Hanna
- The Child Protection Officer : Mr. D. McVeigh
- ICT Coordinator :
- E- Safety Staff Representative :
- ICT technition : Alana Gordan

Members of the Online Safety Team will assist the Online Safety Coordinator with:

- The production and review of the school Online Safety policy and related documents.
- mapping and reviewing the Online Safety curricular provision, ensuring relevance, breadth and progression
- monitoring incident logs from the pastoral team
- consulting parents/carers and the pupils about the Online Safety provision

4.4 The Principal and Senior Leadership Team:

The Principal has a duty of care for ensuring the safety (including Online Safety) of members of the school community though the day-to-day responsibility for Online Safety will be delegated to the SLT and IT Technician.

The Principal/Vice Principal and IT technician will be kept informed about Online Safety incidents.

The Principal will deal with any serious Online Safety allegation being made against a member of staff.

The Principal and SLT are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

4.5 Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports.

reports to the Governors on Online Safety matters..

The designated Online Safety Governor is _____. He/She will:

- have regular meetings with the Online Safety Coordinator
- regularly monitor Online Safety incidents logs
-

Training will be given to the Governors by:

- Attendance at training provided by relevant external agencies / staff in school
- Participation in school's training / information sessions for staff or parents

4.6 Network Managers - Principal/A. Gordon

The Network Managers will monitor that C2K Online Safety measures, as recommended by DENI, are working efficiently within the school.

- that C2k operates with robust filtering and security software
- that monitoring reports of the use of C2k are available on request
- that the school infrastructure and individual workstations are protected by up to date virus software.
- that the school meets required Online Safety technical requirements that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed the filtering policy is applied and that its implementation is not the sole responsibility of any single person that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- that the "administrator" passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place

4.7 Teaching and Support Staff

The Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- They have read, understood and signed the school's Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the Online Safety Coordinator.
- Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School's guidance.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Staff understand and follow the school Online Safety Policy and Acceptable Use Policy.
- That students have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998)
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of Online Safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- Undertake all Online Safety training as organised by the school

4.8 Professional Development for Teaching and Support Staff

Training will be offered as follows:

- All new staff will receive Online Safety training as part of their Induction Programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.
- A programme of Online Safety training will be made available to staff as an integral element of CPD. Training in Online Safety will be supported within the PRSD or EPD process and where staff have identified a need.
- Staff will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

4.9 Pupil Online Safety Committee

The pupil Online Safety committee (sub-committee of the School Council) will assist the Online Safety Officers with:

- Potential issues regarding Online Safety
- Present information during an assembly on the Safer Internet Day
- Pupils will only be expected to take part in staff committee meetings where deemed relevant.

4.9.1 Pupils

Are responsible for ensuring that:

- They use the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to schools systems.
- They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They know and understand school policies on the use of mobile phone, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Pupils are introduced to email and taught about the safety and ‘netiquette’ of using e-mail both in school and at home
- They understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school’s Online Safety Policy covers their actions out of school, if related to their membership of the school.

4.9.2 Online Safety Education for Pupils

Online Safety education for student will be provided in the following ways:

- A planned Online Safety programme will be provided as part of ICT / PHSE / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources will be used as a teaching tool.
- Pupils will be taught in all relevant lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.
- Pupils will be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

4.9.3 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the Online Safety policy outlined by the School.

Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- online communication with staff
- their children's personal devices in the school

4.9.4 Parents / Carers Training and Support

Parents and carers have essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and carers through:

- Parent workshops may be provided digitally
- A section of the school website will provide links to external sites such as CEOP, INEQUE and Digital Parenting
- Letters, newsletters, websites, Edtap
- Online Safety Guidance will be delivered through key events

4.9.5 Education for the Community

- The school will provide opportunities for members of the community to gain from the school's Online Safety knowledge and experience through:
- Providing family learning courses in use of new digital technologies, digital literacy and Online Safety
- The school website
- Supporting community groups e.g. library staff/sports/voluntary groups to enhance their Online Safety provision
- Supporting other local schools and communicating with them to mutually enhance Online Safety provision.

5. Current Practice

5.1 Communication

- The official school email service may be regarded as safe and secure. Staff and pupils should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Email communications with parents and/or pupils should be conducted through the following school email systems '@c2kni.net' Personal email addresses should not be used.

- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers - email, and official school social media accounts - must be professional in tone and content. When emailing, staff should CC any communication to pupils to another member of staff.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

- Further information is provided to staff during in service training, also see the 'Acceptable Use Policy' for appropriate use.

5.2 Social Networking

At present, the school endeavours to deny access to social networking sites to pupils during school hours. Staff may use various medias to disseminate information to pupils outside of school.

- The school will provide training in the appropriate use of social networking / for teaching and learning purposes.
- Training will include: acceptable use; social media risks; checking of settings; data protection; reporting issues; legal risks.
- Teachers should adhere to the social networking / communication guidance provided by the school.
- Teachers will receive training in the appropriate use of social networking in their private life
- Older students should be made aware of the appropriate and safe use of Social Networking
- Teachers and pupils should report any incidents of cyber-bullying to the school.
- Further information is provided to staff during in service training, also see the 'Social Media Policy' for appropriate use.

5.3 Pupils' use of personal devices

- Mobile Phones and personally-owned devices must not be used in school without prior permission from the principal.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Further information is provided to staff/pupils/parents during in service training, also see the 'ICT Policy' for appropriate use.

5.4 Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

- When using digital images, staff informs and educates pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. Social Networking websites.
- The school gains parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those image.
- We will also ensure that when images are published that the young people cannot be identified by the use of their names, unless prior consent has been obtained.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- The use of digital / video images plays an important part in learning activities.
- The school will comply with the General Data Protection Register (introduced May 2018) by requesting parents' permission when their child starts school Year 1, permission will last until the student leaves school, unless a parent / carer provides a written withdrawal of taking images of members of the school.

5.6 Teaching and Support Staff: Password Security

Password security is essential for staff, particularly as they are able to access and use student data.

- Staff are expected to have secure passwords which are not shared with anyone.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.
- Further information is provided to staff during INSET training.

5.7 Students: Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Acceptable Use Policy
- Students are expected to keep their passwords secret and not to share with others, particularly their friends.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

5.7 Cyber-bullying

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Messaging Apps and Forums – 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.
- Incidents of cyber–bullying will be dealt with in accordance with the School Anti-Bullying Policy.

5.8 The Data Protection Act

The school is working towards GDRP compliant status (September 2017).

The school has a Data Protection Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media, it is advisable that:

- the device is password protected
- the device offers approved virus and malware checking software
- the data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete

5.9 Google Apps for Education

The school uses Google Apps for Education for staff. The following services are available to each member of staff and hosted by Google as part of the school's online presence in Google Apps for Education:

- Mail - an individual email account for school use managed by the school
- Calendar - an individual calendar providing the ability to organise schedules, daily activities, and assignments
- Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
- Sites - an individual and collaborative website creation tool
- Drive – an online storage facility used for storing documents and collating portfolios of evidence of T&L.

5.9.1 Technical Framework

Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school's filtering policy is held by the Principal and coordinators.

They manage the school filtering by:

- Monitoring reports of the use of C2k is available on request.
- Keep records and logs of changes and of breaches of the filtering systems.
- These changes and breaches should be reported to the Online Safety Coordinator.

Staff and pupils have a responsibility:

- to report immediately to Principal/IT Technician any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Auditing and reporting:

Logs of filtering change controls and of filtering incidents will be made available to:

- Online Safety Committee
- Online Safety Coordinator
- Board of Governors committee
- External Filtering provider / Police on request

7. Actions and Sanctions

Sanctions for the misuse of technology are outlined in the Acceptable Use Policy:

Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Anti-Bullying Policy will be implemented.