St Killian’s College Garron Tower

e-Safety Policy

Mission Statement

“St Killian’s is a Catholic College which strives to achieve excellence for all, within a happy, supportive and stimulating learning community.”

Date Reviewed
18/04/2018
05/02/2019
16/06/2019
04/02/22
18/09/24

CONTENTS

1. RATIONALE

"All schools should have their own e-Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. e-Safety must be built into the delivery of the curriculum. ICT is a compulsory cross curricular element of the revised curriculum and schools must ensure acquisition and development by students of these skills" ***(DENI e-Safety Guidance, Circular number 2013/25)***

It is the responsibility of the College, 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 Colleges are bound. e-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The College 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 e-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 College community who have access to and are users of the College ICT systems, both in and out of the College. In relation to incidents that occur during school hours, we will work with parents, staff and students to ensure e-Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to e-Safety incidents that occur outside of school hours, the College will work with students and parents to keep all students safe and offer educative support where appropriate. e-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 College 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 College, as a result of e-Safety incidents outside of the College, will be dealt with in accordance with College Policies.

3. RISK ASSESSMENT:

21st century life presents dangers including violence, racism and exploitation from which students 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 College to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Students need to know how to cope if they come across inappropriate material or situations online. The College risk assessments should inform the teaching and learning, develop best practice and be referenced in the College's Acceptable Use Policy. ***(DENI e-Safety Guidance, Circular number 2013/25)***

The main areas of risk for the College 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 e-Safety policy is used in conjunction with other College policies as listed in **Appendix A**.

As with all other risks, it is impossible to eliminate those risks completely. It is ~~-~~essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so they have the confidence and skills to face and deal with these risks.

4. ROLES AND RESPONSIBILITIES:

4.1 ICT Coordinator:

The ICT Coordinator leads the e-Safety Committee and takes day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the Colleges policies/documents.

The ICT Coordinator/C2k Manager will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Provide training and advice for staff
- The ICT Department will deliver e-Safety lessons to Year 8 students through discreet ICT classes at KS3 or Year 8.
- Liaise with C2K, iTeach and the College ICT technical staff
- Liaise with the EA and DENI on e-Safety developments
- Liaise with the technical staff

- Receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments
- Meet regularly with Vice Principal and Child Protection Team to investigate abuse of social network sites by students
- 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 or a breach of safety of which the e-Safety coordinator is aware
- Oversees the application of the 360 Degree Safe Mark Award.

4.2 Designated Child Protection Officer/Designated Deputy Child Protection Officer(s):

The Child Protection Officer (and deputies) will be trained in e-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 e-Safety Committee (Appendix B):

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

- ICT Coordinator
- The Child Protection Designated and/or Deputy Designate Teacher(s)
- Principal
- Network Manager
- ICT Technician
- e-Safety Governor

Members of the e-Safety Committee will assist the ICT Coordinator with:

- the production and review of the College e-Safety policy and related documents.
- mapping and reviewing the e-safety curricular provision, ensuring relevance, breadth and progression
- monitoring incident logs from the pastoral team
- consulting parents/carers and the students about the e-safety provision
- monitoring improvement actions identified through use of the 360‰ Safe Self
- review tool

4.4 The Principal and Senior Leadership Team:

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the College community though the day-to-day responsibility for e-safety will be delegated to the e-Safety Officer.
- The Principal and e-Safety Officer will be kept informed about e-safety incidents.

- The Principal will deal with any serious e-safety allegation being made against a member of staff.
- The Principal will provide regular reports on e-Safety including anonymous details of e-Safety incidents to the Board of Governors.
- The Principal and SLT will inform PSNI, Chair of the Board of Governors, CCM and EA should serious e-Safety incidents occur.
- The Principal and SLT are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

4.5 Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-Safety incidents and monitoring reports. Mr Brian McAuley is the e-Safety Governor.

The e-Safety Governor will:

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

Training will be given to the Governors by:

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

4.6 Network Manager:

The Network Manager will monitor that C2K e-safety measures, as recommended by DENI, are working efficiently within the College.

- that C2K operates with robust filtering and security software
- that monitoring reports of the use of C2K are available on request
- that the College infrastructure and individual workstations are protected by up to date virus software.
- that the College meets the required e-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 e-safety technical information in order to effectively carry out their e-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 College ICT system, used by the Network Managers must also be available to the Principal for overview 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 e-safety matters and of the current College e-Safety policy and practices, have read, understood and signed the College's e-Safety Policy, Acceptable Use Policy and Code of Conduct for staff.
- They report any suspected misuse or problem to the e-Safety Coordinator.
- Digital communications with students (email/Virtual Learning Environment (VLE)
- should be on a professional level only carried out using official College systems – C2K. Emails should be sent in accordance with the College's guidance.
- e-Safety issues are embedded in all aspects of the curriculum and other College
- activities.
- 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 College activities.
- They are aware of e-safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current College policies with regard to these devices.
- They undertake all e-safety training as organised by the College.

4.8 Professional Development for Teaching and Support Staff:

Training will be offered as follows:

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

4.9 Student e-Safety Committee:

The student e-safety committee (sub-committee of the School Council) will assist the e-Safety Officers with:

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

4.9.1 Students:

All students are responsible for ensuring that:

- They use the College ICT systems in accordance with the Internet Acceptable Use Policy, which they will be expected to sign before being given access to the College 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 College policies on the use of mobile phone, digital cameras and hand held devices. They should also know and understand College policies on the taking/use of images and on cyber-bullying.
- They must adhere to the Student Code of Conduct agreement which is signed when the student enrols at the College.
- Students are introduced to e-mail and taught about the safety and the 'netiquette' of using email both in the College and at home
- They understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's e-Safety Policy covers their actions out of College, if related to their membership of the College.

4.9.2 e-Safety Education for Students:

e-Safety education for students will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT/Pastoral Programme/other lessons and will be regularly revisited. Outside agencies, where appropriate, will be involved and with the e-Safety Committee will cover both the use of ICT and new technologies in College and outside the College. Child Exploitation and Online Protection (CEOP) resources will be used as a teaching tool.
- Students 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.
- Students will be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students will be made aware of the importance of filtering systems through the e-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 e-Safety policy outlined by the College.

- Parents and carers will be encouraged to support the College in promoting good e-Safety practice and to follow guidelines on the appropriate use of:
- digital and video images taken at College events
- online communication with staff
- their children's personal devices in the College

4.9.4 Parents/Carers Training and Support

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The College 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 College will seek to provide information and awareness to parents and carers through:
- A section of the College website which will provide links to external sites such as CEOP and Digital Parenting.
- Letters, newsletters, websites.
- e-Safety Guidance will be delivered through key events.
- A designated e-Safety Parents' Evening as part of Induction Evenings.

5. CURRENT PRACTICE:

5.1 Communication:

The official College email service may be regarded as safe and secure. Staff and students should therefore use the College email service to communicate with others when in College, or on College systems (e.g. by remote access).E-mail communications with parents and/or students should be conducted through the following:

- College e-mail systems '@c2kni.net' or @stkillians.carnlough.ni.sch.uk.
- Personal e-mail 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 students or parents/carers – e-mail, VLE and official College social media accounts, must be professional in tone and content. When e-mailing, staff should cc any communication to students to another member of staff.
- Personal information should not be posted on the College website and only official e-mail addresses should be used to identify members of staff.

5.2 Social Networking:

- The College endeavours to deny access to social networking sites to students during College hours.
- Staff may use Twitter/You Tube/VLE/Showbie to disseminate information to students outside of school.
- The College 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 College.
- Teachers will receive training and guidance, on Staff Training Days, 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 students should report, as per the Positive Behaviour Policy, any incidents of cyber-bullying to the College.

5.3 Students' use of personal devices:

The College accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- Mobile Phones and personally-owned devices must be switched off or switched to 'silent' mode', as per the Mobile Phone Policy. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If a student breaches the College policy, then the phone or device will be confiscated and will be held in a secure place in the College office. Mobile phones and devices will be released to parents or carers in accordance with the College Mobile Phone policy.
- In accordance with JCQ regulations, phones and devices must not be taken into
- examinations.
- Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Students 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 College policy, then disciplinary action may be taken.
- Further information is provided to staff/students/parents during in service training.

5.4 CCTV:

The College has CCTV in the College as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission, except where disclosed to the police as part of a criminal investigation.

5.5 Digital and Video Images:

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students 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 students 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 College gains parental/carer permission annually for use of digital photographs or video involving their child as part of the College's positive promotional activity.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images.
- In line with Child Protection Guidelines, the College will also ensure that when images are published that the young people cannot be identified by the use of their names

- Students must not take, use, share, publish or distribute images of other without their permission.
- The use of digital/video images plays an important part in learning activities.
- The College will comply with the Data Protection Act by requesting parents' permission when their child starts school Year 8, permission will last until the student leaves school, unless a parent/carer provides a written withdrawal of taking images of members of the College.

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 College 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.

5.7 Students: Password Security:

- All users read and sign an Acceptable Use of the Internet Agreement to demonstrate that they have understood the College's Acceptable Use Policy.
- Students are expected to keep their passwords secret and not to share with others,
- particularly their friends.
- Students are not allowed to deliberately access on-line materials or files on the College network, of their peers, teachers or others.
- Students are taught about appropriate use of passwords in Year 8.

5.8 Cyber-bullying:

Cyber Bullying can take many different forms and guises including:

- E-mail – 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.
- Incidents of cyber–bullying will be dealt with in accordance with the College Anti-
- Bullying Policy.

5.9 The Data Protection Act:

The College has a Data Protection Policy and staff are regularly reminded of their responsibilities and accountability. 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 College policy once it has
- been transferred or its use is complete.

5.10 Google Apps for Education:

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

- Mail - an individual e-mail account for College use managed by the College
- Calendar - an individual calendar providing the ability to organise schedules, daily
- activities, and assignments
- Docs - a word processing, spread sheet, drawing, and presentation toolset that is
- very similar to Microsoft Office Sites - an individual and collaborative website creation tool

As part of the Google terms and conditions schools are required to seek parental permission for your child (under 13 years old) to have a Google Apps for Education account which will be sought at the beginning of Year 8.

6. 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 College's filtering policy is held by Senior Leadership Team.

They manage the College filtering by:

- Monitoring reports of the use of C2K which are 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 e-Safety Coordinator.

Staff and students have a responsibility:

- to report immediately to e-Safety Coordinator any infringements of the College'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:

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

APPENDIX A

College Policies for reference, to be read in conjunction with e-Safety Policy.

1 Alcohol Policy

2 Anti-Bullying Policy

3 Child Protection /Safeguarding Policy

4 Code of Conduct Policy Guidelines for Staff

5 Code of Conduct Policy for Students

6 Complaints Policy

7 Data Protection Policy

8 Disposal of Records Policy (Schedule)

9 Drugs Policy

10 Internet Policy

11 Mobile Phone Policy

12 Pastoral Care Policy

13 Positive Behaviour Policy

14 Relationships and Sexuality Education Policy (RSE)

15 Special Educational Needs Policy (SEN)

16 Smoking Policy

APPENDIX B

e-Safety Committee 2025

Head of ICT	**Mr Aodhan McAfee**
ICT Co-ordinator	**Mr Peter Marrs**
Designated Child Protection Officer	**Mrs Eileen McKay**
Deputy Designated Child Protection Officers	**Mrs Bernie Haughey** **Mr Dermot Logue**
Principal	**Mr Jonny Brady**
C2K Network Manager	**Mr Dermot Logue**
ICT Technician	**Mr Alvyn McQuitty**
e-Safety Governor	**Mr Brian McAuley**