Saint Catherine's College, Armagh
Coláiste Chaitríona, Ard Mhacha

Digital Safety Policy

The Digital Safety Policy

This Digital Safety policy relates to other major school policies, which can be viewed on the school's website, and include:

- Child Protection Policy
- Anti-bullying Policy
- Acceptable Use of the Internet Policy
- Bring Your Own Device to School Policy
- Mobile Phone Policy
- Positive Behaviour Policy
- Staff Code of Conduct
- Complaints Policy

It has been written by the school's Pastoral Vice Principal in conjunction with the Head of Computing, ICT Network Manager, Designated Teacher for Child Protection and SeniorTeacher in Charge of E-Learning

The Pastoral Vice Principal will also act as the school's designated CEOP Ambassador.

The policy has been agreed by the Senior Leadership Team and approved by the Board of Governors.

The Digital Safety policy and its implementation will be reviewed annually.

Aims of the policy

The aim of this Digital Safety policy is to ensure that pupils will benefit from learning opportunities offered by the school's electronic resources in a safe and effective manner. Digital safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It 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.

Digital safety depends on effective practice at a number of levels:

- sound implementation of an agreed, comprehensive safety Digital policy, in both administration and curriculum
- education for responsible ICT use by staff, pupils and families
- safe and secure broadband, including the effective management of filtering

The Internet is an essential element in 21st century life for education, business and social interaction. Internet use is part of the statutory curriculum and is a necessary tool for both staff and pupils. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet is used in school:

- to enhance the school's management functions
- to support the professional work of staff
- to promote pupil achievement
- to raise educational standards

Computer Network Security

The C2K network used in St Catherine's College is managed and maintained by the C2K support team in the EA along with Capita who is responsible for the hardware and the security of the system.

The following protocols are enforced by the school to comply with security regulations:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly. Portable media will be scanned with anti-virus / malware software. Any device which has a virus will be denied access.
- Unapproved software will not be allowed in work areas or attached to email. Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularity. The use of user Logins and passwords to access the school network will be enforced.

Internet Filtering

- The sole internet provider for pupil use in Saint Catherine's College is the C2k connection. Pupils who access the Internet using eg 3G, 4G, VPNs or other broadband connections while in school are in breach of the school rules. The school's Positive Behaviour Policy will be followed.

The C2k Internet filtering system has a filtering system which provides an effective defence against inappropriate websites. C2K define three types of access:

GREEN accessible to all users in schools

AMBER accessible to school's selected groups of users (can be changed by the C2K Manager)

RED not accessible to any user

An Internet filtering service, no matter how thorough, can never be completely comprehensive. To deal with this issue the school enforces the following rules/procedures:

- Internet sessions will be supervised by a member of staff where possible.
- Pupils' Internet usage is regularly monitored
- Pupils will be aware that any usage, including distributing or receiving information, may be monitored for unusual activity, security and/or network management reasons.
- Pupils will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

- Pupils and staff will report accidental accessing of inappropriate materials in accordance with school procedures.

If staff or pupils discover unsuitable sites, the URL will be reported to the C2K Manager or the Network Manager who will then inform the C2K filtering team to block this website.

Social Networking sites such as Facebook, Instagram, Twitter and Snapchat are all blocked by the C2K Internet filter. However, due to the educational value of Wikis and Blogs, chat rooms, forums and newsrooms in certain subjects, some approved sites can be accessed by a discrete group of pupils who are identified by the Teacher in Charge of e Learning and whose Internet activity is closely monitored.

Staff are advised and given technical support to help set up a secure Wiki and Blog within school and are shown how to monitor the site appropriately.

All pupils who use social sites such as Twitter, Facebook and Blogger within school are asked to sign an acceptable use contract and are assigned usernames and passwords by the relevant teacher to ensure security. Access to the Wiki or Blog within school is strictly for educational purposes only and anyone wishing to join the workspace who is not an approved member by the teacher moderator will be denied.

The school will work with the C2K team to ensure that the filtering policy is continually reviewed.

Teaching and Learning

Through the school curriculum and discrete ICT classes pupils will be taught:

- About acceptable Internet use and practice that is not acceptable
- How to make effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation
- About the importance of acknowledging the source of information derived from the Internet and to respect copyright when using such material in their own work.
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- How to report inappropriate Internet content

This is monitored regularly by the Principal and relevant teams.

Email

Email is an essential means of communication for both staff and pupils for school related business only. The school uses the approved filtered email service provided by C2K. E-mails containing offensive material will be immediately investigated in accordance with other related school policies and may involve outside agencies. The following email procedures are enforced in school:

- C2k email accounts on non-C2k devices must have a lock on them to prevent access to C2k emails by non- C2k users.
- Pupils and staff will not send or receive any material that is offensive, obscene or defamatory or that is intended to annoy or intimidate another person.
- Pupils must immediately tell a member of teaching staff if they receive offensive email. Staff should report such an incident to the appropriate member of staff.
- Staff should only use their school email account to communicate with pupils and parents.
- Pupils and staff will not reveal their own personal details or those of others in e-mail communication.
- Pupils will be encouraged not to arrange a face to face meeting with someone they only know through emails or the Internet.
- Pupils will be taught how to deal with incoming mail and associated attachments.
- Pupils will note that sending and receiving email attachments is subject to permission from their teacher.

Social Networking

This should be read in conjunction with the school's Staff Code of Conduct.

Social networking sites can connect people with similar or different interests but can also pose a number of dangers. All staff and pupils will be made aware of the potential risks of using social networking sites outside of school. They will be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their status.

The following guidance is given to all members of the school community regarding the use of social networking sites which should only be accessed outside of school hours:

- The use of social network spaces outside school is illegal and deemed to be inappropriate for pupils under the age of 13
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications
- Pupils should never give out personal details which may identify them, their friends and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils are advised to use nicknames and avatars(icons or computer characters)when using social networking sites
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private
- All members of the school community are advised not to publish specific and detailed private

thoughts, especially those that may be considered threatening, hurtful or defamatory or bring the name of St Catherine's College into disrepute. Criminal proceedings may be brought to bear in cases where this rule has been contravened.

- Concerns regarding pupils' use of social networking, social media and personal publishing sites (out of school) will be raised with their parents/carers if it impacts on the school community.
- Staff educational Blogs or Wikis should be password protected and monitored very closely. Any breach in security or inappropriate material being published should be immediately reported to the Senior Management Team
- Staff's personal use of social networking, social media and personal publishing sites will be discussed as part of staff training days and will be outlined in the Staff Code of Conduct.

Cyber bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone"

Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying. There are clear procedures in place to support anyone in the school community affected by cyber bullying:

- All incidents of cyber bullying reported to the school will be recorded.
- All incidents or allegations of cyber bullying will be fully investigated.
- Pupils, staff and parents/carers will be advised to keep a written record of the bullying as evidence.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's digital safety ethos.

Personal Electronic devices

Mobile phones and other Internet enabled personal devices can be used to communicate in a variety of ways. Mobile phones, in particular, can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged
- Their use can render pupils or staff subject to cyber bullying
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

The school employs a strict policy on the use of mobile phones on school premises between 8.50 am. and 3.25 pm. Guidelines and sanctions are outlined in the school's Mobile Phone policy. The following

points outline the e safety guidelines for mobile phones/personal devices:

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy and may also be a criminal offence.
- The streaming of online content from sites such as Netflix is strictly prohibited.
- Mobile phones and personal devices will not normally be used during lessons or formal school time unless under the direction of a member of staff for educational purposes.
- The Bluetooth function of all devices should be switched off at all times and not be used to send images or flies to other devices.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. Limited storage facilities are available to Sixth Form students in the Sixth Form Study, Callan Building, but the school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils' Use of Personal Devices

This should be read in conjunction with the school's Mobile Phone Policy and Bring Your Own Device to School Policy which are available on the school website, and whose main points of note include:

- If a pupil breaches the school's Digital Safety Policy regarding personal devices then the phone or device will be confiscated by a member of staff and will be held in a secure place in one of the school's offices. Personal devices will be released in accordance with the school policy. If a potential criminal offence is suspected, the PSNI may need to be contacted.
- Phones and devices such as Apple watches must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone in one of the school's offices. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed (through the ICT Curriculum) in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children or young people.
- Staff should use only the school's landline, or in the case of educational visits, the school mobile phone, where contact with pupils or parents /carers is required.
- Mobile Phones and devices will be switched off or switched to 'silent' mode. Bluetooth communication should be "hidden" or switched off and mobile phones or devices should not be used during teaching periods unless permission has been given by a member of Senior Management in emergency circumstances.

- If members of staff have an educational reason to allow children to use a school issued device as part of an educational activity, then it will only take place when approved by Senior Management.

This guidance is a means of protecting both staff and pupils against unwarranted allegations

Published content and the school website

- The contact details on the website are the school address, e-mail and telephone and fax numbers only.
- Personal pupil and staff information including home address and contact details will be omitted from school web pages
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- Written permission from parents/carers is obtained before photographs of pupils are published on the school website.
- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Any material used by the school will be in keeping with the school's Child Protection Policy.

Virtual Learning Environment (Google Classroom / G-Suite)

An effective virtual learning environment can offer a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

The Virtual Learning Environment (VLE) is subject to careful monitoring by the Head of ICT

- The Head of ICT and staff will regularly monitor the usage of the VLE by pupils in all areas, in particular message, communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the VLE
- All users will be mindful of copyright issues and will only upload appropriate content on to the VLE

Any concerns about content on the VLE may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the VLE for the user may be suspended.

- A pupil's parent/carer may be informed and appropriate outside agencies contacted.

Google Classroom and Collaborate are two of the paperless classroom environments which are extensively promoted by staff for educational purposes. Access to both of these sites can only be approved via a classroom code/link provided by the teacher; parents / guardians can regularly monitor the learning materials on these sites via their daughter's / son's login details. Google classroom is part of the C2k Google Apps for Education suite and so is protected by the C2ken.net login details.

Video Conferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures. The following guidelines must be adhered to when using the video conferencing facilities within school:

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the C2K broadband network should use the recommended conferencing software available in the managed system.
- Videoconferencing contact information will not be published on the school website.
- The equipment must be secure and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.

Users

- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- All teachers are given access to videoconferencing administration areas or remote control pages and are subject to monitoring by C2k.

Content

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate to the class.

Authorising Internet access Digital

- All parents/carers will be asked to read the Digital Safety Policy, discuss it with their child, sign and return the attached agreement form to the school.
- **Parents who do not wish for their child to have access to the Internet in school are asked to indicate this on the relevant section of the agreement form.**
- The school will maintain a current record of all pupils to whom access to school ICT systems is withheld as per signed parental/pupil agreement forms.
- All pupils will read the Digital Safety Policy and sign a Digital Safety Agreement form indicating that they are aware of the rules of conduct when using the Internet and other ICT facilities in the school.

Handling Digital safety complaints

- All members of the school community will be informed about the procedure for reporting digital safety concerns (such as breaches of filtering, cyber bullying, illegal content etc.).
- All incidents and actions concerning e-safety will be recorded.
- The school will manage digital safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- Complaints of a child protection nature must be investigated in accordance with the school's Child Protection policy and will be led by the Designated Teacher for Child Protection.
- The school will inform parents/carers of any incidents of concerns as and when required.
- Any complaint about staff misuse must be referred to the principal.
- Parents will be informed of the school's Complaints Policy, available on the school website.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Sanctions

Misuse of the Internet/electronic resources or damage to the school's good name may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school will report any illegal activities to the appropriate authorities.

Please review the attached Digital Safety Agreement, sign and return to your child's Form Teacher.

Parental Digital Safety Agreement

Name of pupil: _____

Class: _____

As the parent/legal guardian of the above named pupil, I confirm that I have read and agree with the school's Digital Safety Policy. I understand that any breach of the school's Digital Safety Policy could result in a withdrawal of the facility/other disciplinary action.

I also give permission for my child's photograph/work to be published on the school website.

Parental signature: _____

Date: _____

(Only to be completed if you do not wish your child to have Internet access)

I do not grant permission for my child to be given access to the school's Internet systems and understand that this may restrict their learning opportunities.

Parental signature: _____

Pupil Digital Safety Agreement

Name of pupil: _____

Class: _____

As a pupil of St Catherine's College, I confirm that I have read and agree with the school's Digital Safety Policy and understand it is to keep me, my family and friends safe. I understand that any breach of the school's Digital Safety policy could result in a withdrawal of the facility/other disciplinary action.

I agree to follow the school's Digital Safety Policy on the use of the Internet and to use the Internet in a safe and responsible way.

Pupil signature: _____

Date: _____