



# St Columban's College

## E-SAFETY POLICY

### AIMS OF THE POLICY

The aim of this E-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. E-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.

E-safety depends on effective practice at a number of levels:

- sound implementation of an agreed, comprehensive E-safety 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.

The Internet is used in St Columban's College :

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

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

### COMPUTER NETWORK SECURITY

The C2K network used in St Columban's College is managed and maintained by the C2K support team in the SELB 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 regularly.
- The use of user Logins and passwords to access the school network will be enforced.

### INTERNET FILTERING

The school uses the C2K Internet 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
RED	not accessible to any user

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

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 who will then inform the C2K filtering team to block this website. 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

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

### 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:

- Pupils may only use approved C2K email accounts under supervision by or permission from a teacher. The school reserves the right to monitor all email. Access to other email accounts will be blocked.
- Pupils and staff will not send or receive any material that is offensive, obscene or defamatory or that is intended to annoy or intimidate (*cyberbullying*) another person.
- Pupils must immediately tell a member of staff if they receive offensive email. Staff should report such an incident to the Principal.
- 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.
- Pupils must not make use of electronic communication devices to send/receive inappropriate/illegal messages.

### SOCIAL NETWORKING

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

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

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.

Social Networking sites such as Facebook, Bebo, Twitter and MySpace are all blocked by the C2K Internet filter.

Access to Wikis 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 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 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

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

- 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 Columban'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.
- Pupils who access social networking sites blocked by C2K on their mobile phones during school hours are in breach of the school rules. The school's positive behaviour policy will be followed
- 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

### CYBERBULLYING

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.

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-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 cyberbullying
- 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 9.00am. and 3.15 pm. 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 E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

- 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/video etc to other devices.
  
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. 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

- If a pupil breaches the school's E 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 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.

*The E - Safety policy and its implementation will be reviewed annually.*





# St Columban's College

## E-SAFETY POLICY

- 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 E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

- 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 (MOODLE)**

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 in St Columban's College is subject to careful monitoring by the ICT Department. ICT staff will regularly monitor the usage of

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

the College 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.

### AUTHORISING INTERNET ACCESS

- All parents/carers will be asked to read the E-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 E-Safety Policy and sign an E-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 E-SAFETY COMPLAINTS

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

- All members of the school community will be informed about the procedure for reporting e-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 e-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 inappropriate activities to the appropriate authorities. Furthermore, where any breaches of our E-Safety policy, as outlined above, include illegal use of digital technology the cases will be referred to the PSNI.**

*The E - Safety policy and its implementation will be reviewed annually.*



# St Columban's College

## E-SAFETY POLICY

### PARENTAL E-SAFETY AGREEMENT

Pupil:

Class:

As the parent/legal guardian of the above named pupil, I confirm that I have read and agree with the school's E-Safety Policy. I understand that any breach of the school's E-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 or any other school publication.

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:  Date:

### PUPIL E-SAFETY AGREEMENT

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

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

Parental signature:  Date:

*The E - Safety policy and its implementation will be reviewed annually.*