St Louise's
Comprehensive College, Belfast
A Specialist College

E-Safety Policy

ST LOUISE'S MISSION STATEMENT

"In partnership with parents, guardians, staff, governors and students St Louise's promotes excellence in learning and teaching within a Catholic, Vincentian, Comprehensive ethos"

Guidance taken from DE Circular Number 2013/25 and DE Circular Number 2016/27

What is eSafety?

- eSafety is short for electronic safety.
- It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. eSafety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

Overview of Policy

This policy applies to all members of the school community including:

- ✓ Permanent Staff both teaching and non-teaching
- ✓ Temporary staff including volunteers
- ✓ Students
- ✓ Parents/Carers
- ✓ Visitors who have access to and are users of school ICT systems, both in and out of school.

SECTION 1
RAISING AWARENESS OF ALL STAKEHOLDERS

Raising Awareness for Students

The education of students in e-safety is an essential part of the school's e-safety provision. Students will be given help and support within school to recognise and avoid e-safety risks and build their resilience. They will be taught how to respond to risks appropriately.

E-Safety education within St Louise's is provided in the following ways:

- ✓ A planned e-safety programme should be provided as part of ICT lessons and Year Team Induction at the beginning of each academic year;
- ✓ Key e-safety messages will be reinforced as part of our Safeguarding Curriculum at Whole School Level;
- ✓ Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
- ✓ Students will be helped to understand the need for the student AUP as part of their Induction Programme and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- ✓ Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- ✓ Rules for use of ICT systems/internet will be posted in all rooms; and
- ✓ Staff will act as good role models in their use of ICT, the internet and mobile devices.

Raising Awareness for Parents

The school will provide information and awareness to parents and carers through:

- ✓ Letters, newsletters, web site, text messages, VLE
- ✓ Parents evenings
- ✓ Regular letters

Raising Awareness for Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- ✓ A planned programme of formal e-safety training programme through the development of a revised pastoral programme for students will allow for training by the E-learning co-ordinator in August 2017;
- ✓ All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies;
- ✓ The E-Learning Coordinator will receive regular updates through attendance at courses and reviewing guidance documentation;
- ✓ This E-Safety policy and its updates will be presented to and discussed by staff when required; and
- ✓ The E-Learning Coordinator/ICT Manager will provide advice, guidance and training to individuals as required.

Raising Awareness for Governors

Governors will take part in e-safety training / awareness session. This may be offered in a number of ways:

- ✓ Attendance at training provided by EA/C2K.
- ✓ Participation in school training / information sessions for staff or parents

SECTION 2
ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Board of Governors

The Board of Governors of St Louise's are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Vice Principal in charge of curriculum and Pastoral Care in consultation with the ICT Manager will prepare a yearly report for governors outlining the following:

- ✓ Update on ICT developments
- ✓ Summary of incidents relating to E-Safety

The Principal and Senior Leadership Team

- ✓ The Principal is responsible for ensuring the safety (including e-safety) of members of the school community. However, day to day responsibility for e-safety will be

delegated to the Vice Principals in charge of Curriculum and Pastoral Care, E-Learning Co-ordinator and ICT Manager.

- ✓ The Vice Principals in charge of curriculum and Pastoral Care are responsible for ensuring that the E-Learning Coordinator, ICT Manager and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- ✓ The Senior Leadership Team, Heads of Year and Designated teachers for Child Protection are fully aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Vice Principals in charge of curriculum and Pastoral Care will be supported by the E-learning Co-ordinator in:

- ✓ leading the e-learning team;
- ✓ taking the day to day responsibility for issues and has a leading role in establishing and reviewing the school e-safety policies / documents;
- ✓ ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- ✓ providing training and advice for staff;
- ✓ liaising with school ICT technical staff;
- ✓ collating reports of e-safety incidents and creating a log of incidents to inform future e-safety developments (see Appendix 1a/b – E- safety for Staff/Students);
- ✓ attending relevant meetings outside school;
- ✓ reporting regularly to Senior Leadership Team

The Principal will provide an update to the Board of Governors as issues arise.

ICT Manager

The ICT Manager will be responsible for ensuring that:

- ✓ the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- ✓ the school meets the e-safety technical requirements outlined in the C2K Guidance and Acceptable Usage Policy;
- ✓ users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- ✓ access to other peoples' accounts can only be done with the permission of the Principal. This will only occur where there is an investigation. In all other cases, permission will be sought from the user;
- ✓ the school's filtering policy, is applied and updated on a regular basis though C2K and that its implementation is not the sole responsibility of any single person;
- ✓ he keeps 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 the use of the network, Virtual Learning Environment (VLE), remote access, email are regularly monitored in order that any misuse and/or attempted misuse can be reported to the Principal; and
- ✓ that monitoring software / systems are implemented and updated as agreed in school policies
- ✓ The ICT Manager is the only person who can access the full computer system with the permission of the Principal.

Teaching and Support Staff are responsible for ensuring that:

- ✓ they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- ✓ they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP);
- ✓ they report any suspected misuse or problem to the Head of Year/Member of the Senior Leadership Team with responsibility for the Year Group;
- ✓ digital communications with students through email/Virtual Learning Environment (VLE) should be on a professional level and should only be used for the transfer of information of an educational nature, on equipment provided by the school, not on their personal equipment;
- ✓ e-safety issues are embedded in all aspects of the curriculum and other school activities;
- ✓ students understand and follow the school e-safety and acceptable use policy;
- ✓ students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- ✓ they monitor ICT activity in lessons, extra-curricular and extended school activities;
- ✓ they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices; and
- ✓ in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Such processes are in compliance with the school's safeguarding/Child Protection policy. All materials used

must be age appropriate and in line with the ethos of the Catholic School.

Designated and Deputy Designated Teacher for Child Protection

Training will be provided linked to e-safety issues and the designated teachers will be aware of the potential for serious child protection issues to arise from:

- ✓ sharing of personal data;
- ✓ access to illegal / inappropriate materials;
- ✓ inappropriate on-line contact with adults/strangers;
- ✓ inappropriate use of cameras/mobile phones/hand held devices;
- ✓ potential or actual incidents of grooming; and
- ✓ cyber-bullying.

Students:

are responsible for using the school ICT systems in accordance with the Student/Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems;

- ✓ have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- ✓ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- ✓ will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices;
- ✓ should not take or use images of staff and/or students;

- ✓ should be fully aware of the school's policy on cyberbullying; and
- ✓ should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers will play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be responsible for:

- ✓ endorsing (by signature) the Student Acceptable Use Policy; and
- ✓ accessing the school website / VLE / on-line student records in accordance with the relevant school Acceptable Use Policy.

SECTION 3
TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

With support from C2K, the school is responsible for ensuring that the school Infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- ✓ School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy;
- ✓ There will be regular reviews and audits of the safety and security of school ICT system;
- ✓ Servers, wireless systems and cabling must be securely located and physical access restricted;
- ✓ All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the C2K Manager and will be reviewed, at least annually, by the E-Learning Co-ordinator/Vice Principal;
- ✓ All users will be provided with a username and password by the C2K Manager who will keep an up to date record of users and their usernames;
- ✓ The "administrator" passwords for the school ICT system, used by the C2K Manager must also be available to the Principal;
- ✓ Users will be made responsible for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- ✓ The school maintains and supports the managed filtering service provided by C2K ;
- ✓ Any filtering issues should be reported immediately to C2K;
- ✓ Requests from staff for sites to be removed from the filtered list will be considered by the Principal in liaison with the C2K Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Learning Committee;
- ✓ Users will report any actual / potential e-safety incident to a member of the Senior Leadership Team or the Head of Year in charge of the Year Group;

- ✓ Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data;
- ✓ The C2K Manager will grant temporary access of "guests" (eg trainee teachers, visitors) onto the school system in liaison with the Principal;
- ✓ The school infrastructure and individual workstations are protected by up to date virus software; and
- ✓ Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

C2k Advice and Guidance (Circular Number 2013/25) and Circular number 2016/27

The main eSafety elements that Principals, Senior Leadership Teams and Governors need to prepare and plan for the introduction of are outlined in the table on page 13.

Internet Filtering	Improved Websense filtering will give schools the flexibility to control and develop their own internet Filtering Policy. Individual schools may now select to fully delegate management of their filtering policy to a nominated member of staff by signing up to C2k delegated filtering access. This nominated user will receive additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This is in direct response to feedback from schools, who wish to access more internet sites to enhance teaching and learning. However there are a number of agreed locked down sites that can never be overridden by the local school policy.
Meru Wireless	Meru Wi-Fi will provide increased wireless coverage and improved speed. Meru supports multiple devices and school controlled secure guest access and allows schools to plan for and implement a further purchase by the school or/and a 'Bring Your Own Device' policy.
Cloud Storage	Data and information will be stored on the Cloud in the new service and no longer in the school itself. This means it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.
Personal Devices	Schools will be able to explore the introduction of new internet enabled devices to support teaching and learning. These include PCs, Laptops, netbooks, tablets and phones. Control of access to the internet is managed by the school and must be enabled for each device.
Granular Controls	Through the new managerial console, each school C2k Manager will be able to control access to the internet and services to named individuals and groups of users based on their role in the school, their age, courses studied or to support individual needs.

SECTION 4
LEARNING AND TEACHING

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- ✓ In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- ✓ Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- ✓ Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- ✓ Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Grey Filtering within C2k – Key message for Teaching Staff

C2k has created a new filtering group, the Grey Area, which will provide access for staff only, to a number of websites which are currently blocked but which would be considered of value for teaching and learning. Access is restricted to school staff as many of the sites may provide access to inappropriate content.
In asking for access to this filtering group, it is vital that you take note of the following:

- ✓ The sites that are made available may contain inappropriate material – it is expected that any sites being used in the classroom have been checked to ensure that there is no inappropriate content;
- ✓ The list of sites will be added to over time and by asking for access to the group you recognise that all sites listed will be accessible. The list of sites will be kept up to date;
- ✓ As the sites will only be available to staff it is important to emphasise that a computer on which a member of staff is logged onto should not be left unattended. In addition, particular attention should be paid to the security of staff usernames and passwords. A member of staff's logon details should never be given to a student; and
- ✓ Particular care should also be taken when accessing the sites while projecting the sites on a whiteboard, as inappropriate material may be displayed.

Use of digital and video images

- ✓ When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet eg on social networking sites;
- ✓ Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, parental consent must be gained and the personal equipment of staff should not be used for such purposes;
- ✓ Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not

participating in activities that might bring the individuals or the school into disrepute;

- ✓ Students must not take, use, share, publish or distribute images of others without their permission;
- ✓ Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- ✓ Written permission from parents or carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year);
- ✓ Student's work can only be published with the permission of the student/pupil and parents or carers; and
- ✓ Staff must not show videos/DVDs unless for educational purposes or for pastoral rewards; and
- ✓ Staff and students must not use show, use, publish or share materials which contravene the ethos and value system of St Louise's.

Communication between Staff, Parents and Students

When using communication technologies the school considers the following as good practice:

- ✓ Users must immediately report, to the Principal– in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
- ✓ Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official monitored school systems. Personal email

addresses, text messaging or public chat/social networking programmes must not be used for these communications;

- ✓ Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material; and
- ✓ Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- ✓ The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

SECTION 5
UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context or would conflict with the school's ethos, either because of the age of the users or the nature of those activities. Any issues/concern staff may have, they must contact the E-learning Co-ordinator for clarification, who will contact the Vice-Principals/Principal.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these

activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Actions of Users

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
	adult material that potentially breaches the Obscene Publications Act in the UK
	criminally racist material in UK
	pornography
	promotion of any kind of discrimination
	threatening behaviour, including promotion of physical violence or mental harm
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
Using school systems to run a private business	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by C2K and/or the school	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)	
Creating or propagating computer viruses or other harmful files	

Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
On-line gaming (educational)
On-line gaming (non educational)
On-line gambling
File sharing
Use of social networking sites – in instances where this may be used for educational purposes, permission must be sought through the E-Learning Co-ordinator.

Responding to incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate,

preserve evidence and protect those carrying out the investigation.

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