SAINT KEVIN'S COLLEGE

Deo ducente

Est. 2017

- Believe - Achieve - Succeed -

e-Safety Policy

Signature of Chairperson of Board of Governors: ________________

Signature of Principal: __________________________________

Date: __________________________________

Review Date: __________________________________

E-SAFETY POLICY

1. INTRODUCTION

Boards of Governors have a duty to safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries (Northern Ireland) Order 2003). It is also the duty of the Board of Governors to determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003 refers).

In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.

This E-safety policy contains policies in relation to use of the internet, use of mobile phones/handheld devices and use of digital/photographic images of children. It is largely based on DENI Circular 2007/1 “Acceptable Use of the Internet and Digital Technologies in Schools”, DENI Circular 2011/22 “Internet Safety”, DENI Circular 2013/25 “eSafety Guidance” and DENI Circular 2016/17 “Online Safety”. It should also be read in conjunction with the Child Protection Policy.

2. INTERNET SAFETY POLICY

The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The DENI circular 2007/01 states that:

“Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools.”

This document sets out the policy and practices for the safe and effective use of the Internet in St Kevin’s College. The policy has been drawn up by the staff of the school under the leadership of Gary Kelly/Don Callan *(Principal/ICT Co-ordinator)*. It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested.

The policy and its implementation will be reviewed annually.

3. EA/C2K

EA/C2k is responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

Some of these safety services include:

- Providing all users with unique usernames and passwords
- Tracking and recording all online activity using the unique usernames and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses
- Filters access to web sites
- Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

4. Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. We have a Student Internet Contract for pupils (Appendix 1) and ICT Code of Safe Practice for Staff (Appendix 2) containing e-Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, tablets and digital photography/video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones/devices, camera phones, tablets, PDAs) is subject to the same requirements as technology provided by the school.

Don Callan, the ICT Co-ordinator and Gary Kelly /Senior Management Team will monitor the effectiveness of the Student Internet Contract for pupils and ICT Code of Safe Practice for Staff particularly in the light of new developments in technology.

- Code of Safe Practice for Pupils

Parental/carer consent is required before a pupil is given access to the internet. The Student Internet Contract is communicated via form teachers and during initial ICT lessons.

In addition, the following key measures have been adopted by St. Kevin's College to improve the e-safety provision for students:

- Biannual e-safety audit will be completed and reviewed by the ICT coordinator with appropriate actions taken to deal with main areas of concern;
- The school's eSafety code of practice for Use of the Internet and other digital technologies is made explicit to all pupils and eSafety guidelines are displayed prominently throughout classrooms in school;
- Our Code of Practice is reviewed each school year and amended as necessary;
- Securus is used to monitor internet usage.
- Pupils using the Internet will normally be working in highly-visible areas of the school;

- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;
- All pupils are educated in the safe and effective use of the Internet;
- A student led e-safety assembly will be delivered to both KS3 and KS4/KS5 students through the school's form class assembly rota;
- Students will receive guidance from outside agencies where appropriate.

It should be accepted that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances. Children will be asked to inform an adult about any incidents they witness.

The use of mobile phones by pupils for personal reasons is not permitted on the school premises during school hours. During school hours pupils are forbidden to play computer games or access social networking sites. If a teacher feels the use of a phone would be beneficial when delivering a certain aspect of their curriculum it must be approved by their head of department. If phones are being used during lesson it is important their use is supervised and clear guidance on acceptable use is given to the students beforehand. Any student who needs to access the Sims app must do so only with the permission of a member of staff or during break/lunch in permitted phone zones.

- Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Behaviour Policy. Minor incidents will be dealt with by class teachers and Year Heads with the support of D Callan and C O Neill and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's child protection policy.

- Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff:

- Pupils accessing the Internet should be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinator.
- In the interests of system security staff passwords should only be shared with the network manager.
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.

- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.

- Recordings (including still images/moving images and audio) of pupils should only be taken with a school camera/device and files should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work.

- School systems may not be used for unauthorised commercial transactions.

5. Internet Safety Awareness

In St. Kevin's College we believe that, alongside having a written eSafety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils. Securus is used to analyse internet use and potential issues are communicated via reports to the appropriate member of staff (Year Head) and D Callan. This will also enable us to teach the students to make more responsible choices whilst using computers/ the internet.

- **Internet Safety Awareness for pupils**

  Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, pupils are made aware and discuss Internet Safety through structured activities as shared by the ICT co-ordinator. Each month we will have a clear e-safety message which will be introduced by form teachers/year heads and displayed on the screen in reception.

  There are various pupil resources available through the School website such as:

  Gridclub

  Signposts to Safety (primary and secondary versions)

  KidSMART

  ThinkUKnow

  Childnet's Sorted website

  CEOP

  The school Facebook page will also be used to share important information regarding online safety with students when necessary.

- **Internet Safety Awareness for staff**

  The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Departments policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.

The Child Exploitation and Online Protection Centre (CEOP) runs regular one-day courses for teachers in Northern Ireland. These are advertised directly to schools. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the Thinkuknow website.

- **Internet Safety Awareness for parents**

  The school E-Safety policy will be available for download on the school website. Parents can also request a hard copy.

  On the school website there is a dedicated e-Safety page with links to websites and digital tools.

  The school Facebook page will also be used to share important information regarding online safety with parents.

- **Community Use of School ICT Resources**

  The school's ICT facilities are used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by C2K. They must also agree to the school's Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

6. Health and Safety

In St. Kevin's College we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are also mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

- **Wireless Networks**

  The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available at: the Health Protection Agency website.

7. School Web Site

The school website is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Website reflects the school's ethos that information is accurate and well-presented and that personal security is not compromised. An editorial team ensure common values and quality control. As the school's Website can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply:

- The point of contact on the Website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site (see school Pupil Data Collection Form).
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- The ICT co-ordinator and Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

8. Social Software

This is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks, video calling and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.

The majority of activity in these on-line social sites usually causes no concern. C2k filters out these social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment.

We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Appropriate information and indeed education will also be provided for our parents.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school’s discipline policy and child protection procedures.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Use of Student Images/Recording on Social Media

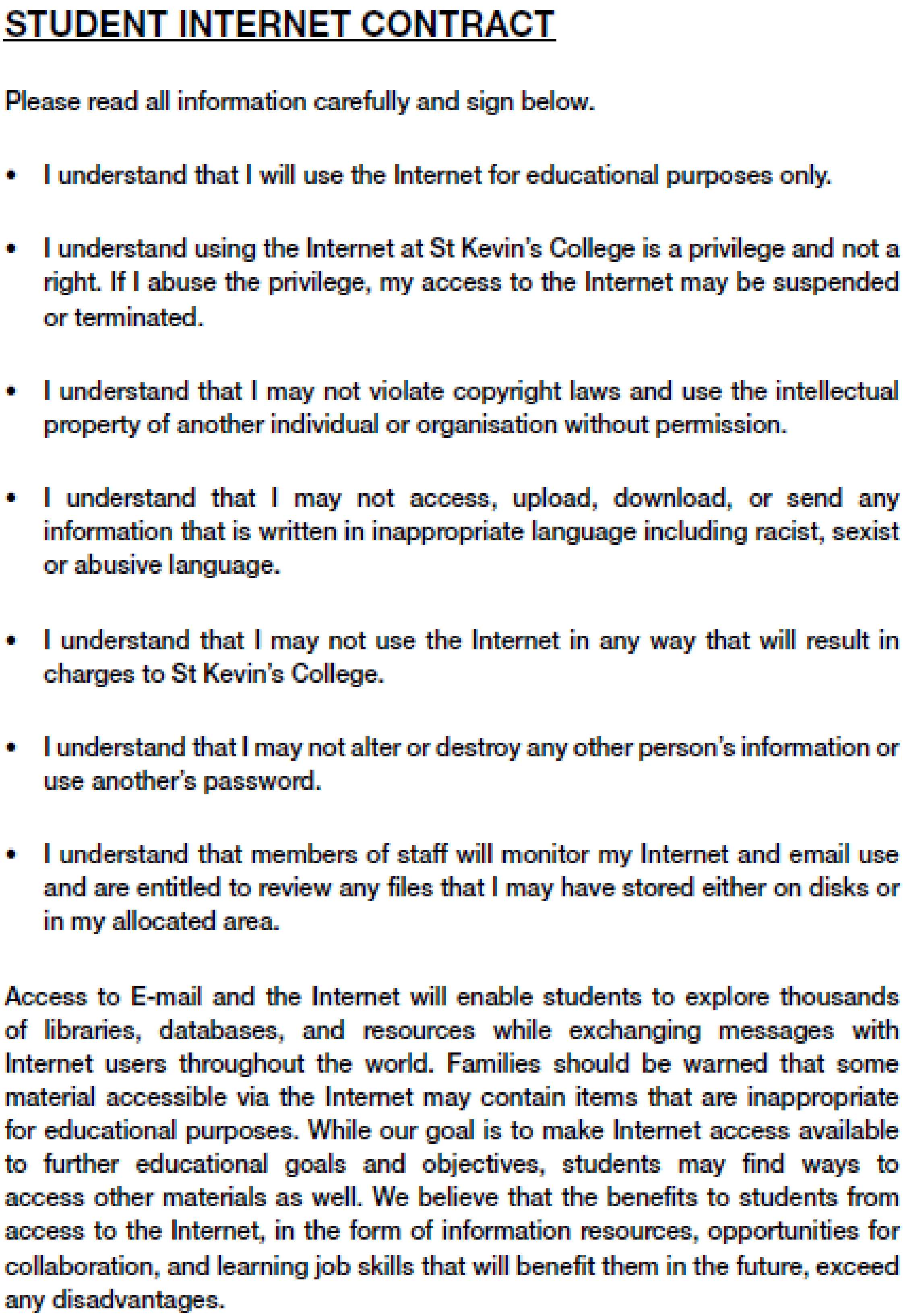
When Public Relations Officer or ICT Technician are taking photos/video/audio involving students all students will be verbally reminded of the purpose of these use and that these may be shared on social media profiles, advertising or in print.

All social media requests from staff are logged through the social media log in order to submit staff must confirm that they have permission to use photos or videos of the students involved.

The PRO and ICT Tech then review requests and if suitable are made up and added to the social media content calendar.

Posts on the calendar are then approved by the Head of Key Stage Four and Five and then and only then scheduled on the school's social media platforms.

Appendix 1



STUDENT INTERNET CONTRACT

Please read all information carefully and sign below.

- I understand that I will use the Internet for educational purposes only.

- I understand using the Internet at St Kevin's College is a privilege and not a right. If I abuse the privilege, my access to the Internet may be suspended or terminated.

- I understand that I may not violate copyright laws and use the intellectual property of another individual or organisation without permission.

- I understand that I may not access, upload, download, or send any information that is written in inappropriate language including racist, sexist or abusive language.

- I understand that I may not use the Internet in any way that will result in charges to St Kevin's College.

- I understand that I may not alter or destroy any other person's information or use another's password.

- I understand that members of staff will monitor my Internet and email use and are entitled to review any files that I may have stored either on disks or in my allocated area.

Access to E-mail and the Internet will enable students to explore thousands of libraries, databases, and resources while exchanging messages with Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are inappropriate for educational purposes. While our goal is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources, opportunities for collaboration, and learning job skills that will benefit them in the future, exceed any disadvantages.

The Internet is provided for students to **conduct research and communicate** with others. Downloading is not allowed, except for school-related files.

Access is a privilege, not a right. Access entails responsibility. It is presumed that users will honour the agreements they have signed. Access will be limited based upon limited time for our Internet accounts and educational considerations. Access to network service is given to students who agree to act in a considerate and responsible manner.

Computer storage areas and disks may be treated like school lockers. **School officials may review files and communications** to maintain system integrity and insure that users are engaging in responsible activities. Users should not expect that files stored on computers and disks will always be private.

Any faculty member involved with the use of computers may, at their sole discretion, reserve the right to **terminate immediately the privileges of any student** who misuses the account.

It can be EXTREMELY DANGEROUS to enter chat rooms, therefore no pupils are allowed to enter them at any time.

Breach of Rules may lead to:

- Suspension of information network privileges;
- Suspension of computer privileges;
- School suspension/expulsion.

....

To gain access to E-mail and the Internet, all students must obtain permission from a parent or guardian and must sign this form.
I have read the above regulations and I agree to abide by them.

Student Signature:________________________________ Date:__________________

I have reviewed these rules with my son/daughter.

Parent Signature:________________________________ Date:__________________

Appendix 2

ICT Code of Safe Practice for Staff

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with D. Callan (ICT Coordinator) or G. Kelly (Principal).

Code of Practice

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.

- I will only use the approved, C2k, secure e-mail system for any school business.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.

- I will not install any hardware or software without first discussing with the ICT technician.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Recordings (including still images/moving images and audio) of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Recordings will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.

- I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, by my Principal.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school.

Signature ………………………………………. Date ……………………

Full Name …………………………………….. (printed)

Appendix 3

Student Mobile Phone Policy

The use of a mobile phone in school is a privilege and the following must be adhered; otherwise the phone will be confiscated and will only be collected from the school by the child’s Parent/Carer.

- I will only use my mobile phone in one of the designated areas (IT Area Main Corridor, Picnic Tables, Canteen, Foyer) or when approval has been granted by a member of staff
- I will only use my mobile phone for educational purposes whilst in school
- I will ensure my mobile phone stays screen up and placed on the top right corner of my desk when I am using it in lesson
- I understand it is my responsibility to charge my phone and that I cannot do this during the school day
- I understand that the taking of photographs is prohibited, unless approved and supervised by a member of staff for educational purposes
- I understand that the recording of audio or video is prohibited, unless approved and supervised by a member of staff for educational purposes
- I understand that it is my responsibility to report any misuse to a relevant member of staff
- I will ensure my mobile phone is turned off when not in use
- I will have a pin on my phone at all times for security purposes.