Our Lady and St Patrick's College, Knock

eSafety and Digital Technology Policy

Policy Details

Legal Status	Adopted	Version Date	Last Review	Next Review	Responsible
Non-statutory	6th June 2019	May 2019	N/A	May 2022	Mr McGrath

Related Documents and Location

1. Anti-Bullying Policy
2. Positive Behaviour Policy
3. Child Protection/Safeguarding Policy
4. DE Annual Child Protection Evaluation
5. Acceptable Use of Digital Technology - Staff (Appendix 1)
6. Acceptable Use of Digital Technology - Students (Appendix 2)

All policies are available on the College Website and Private Folders.

Contents

1. Introduction

The College Mission Statement seeks to:

"*Prepare our students to play an active and responsible role in society*."

In pursuit of this aim, the College is committed to the use of digital technology to improve learning and teaching, using the Education Authority funded C2k Education Network. The College also has a duty of care to enable students to use digital technology safely. Therefore, to ensure the welfare and safety of our College community, all students and staff are expected to adhere to this eSafety and Digital Technology Policy which operates in conjunction with the College's Anti-Bullying Policy, Positive Behaviour Policy and Child Protection/Safeguarding Policy. It also reflects the guidance set out in the DE Circulars listed in Appendix 4 on Page 17 and other relevant UK legislation.

2. Aims

1. To take appropriate preventative action to safeguard students in the digital world.
2. To promote the use of digital technology by students and staff to improve learning and teaching.
3. To emphasise learning to understand and use digital technology in a positive way.
4. To make students aware of the risks as well as the benefits so that they feel confident online.
5. To support students to develop safer online behaviours both in and out of school.
6. To help students recognise unsafe situations and how to respond to risks appropriately.
7. To implement robust filtering and security software for the College network.
8. To monitor reports of eSafety incidents to inform future eSafety developments.

3. Definition of eSafety and Digital Technology

The DENI eSafety Strategy Consultation Document (March 2019) states that:

*"**eSafety** is about using electronic devices in a safe, responsible and respectful way. It means safeguarding children and young people in the digital world and educating them to keep themselves safe online."*

Furthermore, DE Keeping Children Safe in Education (September 2018) states that eSafety can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users;
- conduct: personal online behaviour that increases the likelihood of, or causes, harm. [1]

Digital Technology covers the electronic equipment, networking facilities, online services, digital media and software applications used to create, store, process, analyse and present digital information.

4. Scope of the Policy

This policy applies to all members of the College community who have access to and are users of the College's IT network, both in and out of school. Incidents which occur during school hours which contravene this Policy will be dealt with in accordance with College Policies. eSafety incidents which occur outside school hours are primarily the responsibility of parents. Parents are encouraged to report serious breaches of eSafety outside of school to the PSNI. The College, however, reserves the right to deal with eSafety issues which take place outside of the College and have a detrimental effect on the student's education. It will be at the discretion of the College to determine if any such issue falls within the remit of this policy.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf

5. The eSafety Committee

Designated Governor for eSafety	Ms Jackie Devine
Vice Principal (Pastoral Care)	Ms Grace McCarthy
Senior Leadership Team	Mrs Fiona Knight
ICT Coordinator	Mr Andrew McGrath
IT Manager	Mr Paul Ashe
Year 14 Digital Mentors	Year 14 students x 2

If appropriate, other staff or students may be invited to attend a meeting of the College eSafety Committee.

6. Roles and Responsibilities

6.1 **The Board of Governors** has a duty:

- to safeguard and promote the welfare of all children in the care of their school;
- to ensure that there is an eSafety Policy and that it is implemented;
- to consult with students and parents;
- to address the issue of bullying through discipline policies.

The Board of Governors must ensure that:

- a Designated Governor for eSafety is appointed to the eSafety Committee;
- the College has an eSafety and Digital Technology Policy which is reviewed every 3 years;
- eSafety training is given to all staff;
- the Board of Governors receive a termly report of child protection activities and eSafety matters.

6.2 **The Designated Governor for eSafety** provides advice to Governors about:

- the College's eSafety and Digital Technology Policy;
- the content of eSafety reports;
- any deficiencies in the College's eSafety best practice arrangements as identified by the College eSafety Committee;
- any remedial action taken or recommended to address deficiencies in eSafety practice requirements.

6.3 **The eSafety Committee** assists the ICT Coordinator with:

- the review of the College's eSafety Policy and related documents;
- improvement actions identified through use of the 360 Degree Safe Self-Review Tool;
- mapping and reviewing the eSafety curricular provision in the College;
- monitoring incident logs from the IT Manager;
- consulting students and parents about eSafety provision.

6.4 **The ICT Coordinator** leads the eSafety Committee and takes day-to-day responsibility for eSafety issues. The ICT Coordinator will:

- oversee the application of the 360 Degree Safe Self-Review Tool;
- provide training and advice for students, staff and parents;
- ensure that all students and staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place;
- liaise with C2k and College IT staff;
- Keep up-to-date with the Education Authority, DE and C2k on eSafety developments;
- receive reports of eSafety incidents and create a log of incidents to inform future eSafety developments;
- meet with the Vice Principal (Pastoral Care) to investigate abuse of social network sites by students;
- attend relevant meetings with the Board of Governors;
- monitor and report to the eSafety Committee any risks to students or staff of which the ICT Coordinator is aware.

6.5 **The IT Manager** will ensure that:

- eSafety measures, as recommended by DE, are working efficiently within the College;
- C2k operates with robust filtering and security software;
- the school infrastructure and individual workstations are protected by up-to-date anti-virus software;
- the College meets required eSafety technical requirements that users may only access the networks through properly enforced password protection;
- passwords are regularly changed;
- the filtering policy is applied;
- he keeps up-to-date with eSafety technical information in order to effectively carry out his eSafety role;
- he reports any suspected misuse or a breach in eSafety to the Designated Teacher for Child Protection, ICT Coordinator or Head of Year, as appropriate;
- where appropriate, he reports any breach in eSafety to C2k;
- he monitors Securus and refers any student in breach of Acceptable Use of Digital Technology/deemed to be at risk to his/her Head of Year/the Designated Teacher for Child Protection;
- the eSafety Committee is kept informed and updated as relevant;
- software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- the "administrator" passwords for the College IT systems, used by the IT Manager, are also available to the Principal and kept in a secure place.
- usernames are only available for current staff and students. Additional users, e.g. exam users, guest users and substitute teachers are checked on a regular basis.
- any user under investigation for inappropriate use of the system is disabled promptly.
- all Legacy network servers and desktops must have:
    - adequate, up-to-date anti-virus protection with automatic updates;
    - appropriate, up-to-date security patches and service packs installed.

6.6 **The Designated Teacher(s) for Child Protection** will deal with Child Protection issues arising from:

- the sharing of inappropriate personal data;
- access to inappropriate/illegal materials;
- inappropriate online contact with peers/adults/strangers/others;
- potential or actual incidents of grooming;
- cyberbullying.

6.7 **Staff** must ensure that they adhere to the College's eSafety and Digital Technology Policy - Acceptable Use of Digital Technology - Staff (Appendix 1, Page 10-13).

6.8 **Students** must ensure that they adhere to the College's eSafety and Digital Technology Policy - Acceptable Use of Digital Technology - Students (Appendix 2, Page 14-15).

6.9 **Responsibilities of Parents**

Parents are advised that they are responsible for their children's out-of-school online use of the C2k services and College devices, including the My Documents area, email and Fronter. http://www.c2kschools.net. Parents should ensure that their child complies with the age restrictions on Social Media Services.

7. Security Measures

The C2k Education Network ensures that a range of security measures is in place to secure the College and its users against potential risks. These include: firewalls; intrusion prevention systems; content filtering; email scanning and filtering; secure hosted applications; ongoing vulnerabilities assessment; user authentication using encryption and data security.

8. Email Security

All staff and students are given access to the College's C2k and Gmail email systems. Individual usernames and passwords must be kept private. Staff must not use personal email accounts for school business. 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.

9. Filtering of Internet Access

The Education Authority/C2k provides a filtered Internet service for schools in Northern Ireland. This is provided as part of the core C2kEn NI service in all schools. As a result, the following categories of websites are not, by default, available to users:

- **adult**: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;
- **violence**: content containing graphically violent images, video or text;
- **hate material**: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds;
- **illegal drug taking and the promotion of illegal drug use**: content relating to the use or promotion of illegal drugs or misuse of prescription drugs;
- **criminal skill/activity**: content relating to the promotion of criminal and other activities;
- **gambling**: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

The DE funded C2k Education Network is fully monitored and risk assessed by C2k. A hardwall firewall filter is installed which intercepts all Internet traffic leaving and entering the school network. It is understood, however, that a filtering service, no matter how thorough, can never be comprehensive. If, at any time, students or school staff find themselves able to access inappropriate material which they think should be blocked, they should advise a member of staff/the IT Manager.

10. Securus

The College uses Securus, which forms part of the eSafety suite of tools available to schools via the C2k Education Network, to safeguard children in their use of information systems and electronic communications. Securus monitors the screen display and keystrokes of students on C2k managed devices and triggers a capture if the content is listed in the database of inappropriate words and phrases.

Securus is monitored by the IT Manager. Any student in breach of Acceptable Use of Digital Technology is referred to his/her Head of Year. Students will be subject to sanctions as per the College Positive Behaviour Policy. Any student who opens the College to a serious security breach (virus) will be recommended for suspension.

Any student deemed to be at risk is referred to the Designated Teacher for Child Protection.

11. Procedure for Reporting a Breach in eSafety

- The ICT Coordinator ensures that all students and staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Students report any suspected misuse or a breach in eSafety to a member of staff.
- Staff report any suspected online misuse or a breach in eSafety to the Head of Year or the IT Manager (Mr Ashe), as appropriate;
- The IT Manager reports any suspected misuse or a breach in eSafety to the respective Head of Year, the Designated Teacher for Child Protection or the Principal, as appropriate.
- Where appropriate, the IT Manager reports any breach in eSafety to C2k.
- The ICT Coordinator receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments.

12. Education of Students

The Internet is an integral part of students' lives, both inside and outside school. The College, therefore, actively promotes age-appropriate online safety messages for students on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety. The delivery of this preventative curriculum enables students to experience the benefits of communicating online, in relative safety. eSafety is actively promoted through:

- Specific ICT lessons;
- ICT as a cross-curricular skill;
- Child protection/safeguarding talks;
- Personal Development lessons;
- EFL lessons;
- Mentor lessons;
- Digital Mentor lessons;
- Assembly;
- Safer Internet Day;
- Anti-Bullying Week;
- Focus of the Week.

13. Education of Parents and Other Key Stakeholders

The College aims to make parents, Governors and the wider College community aware of important online safety messages via appropriate training providers. Online safety resources and messages are shared with parents via Communiqué, the College e-bulletin, the College website and social media, where appropriate. DE circulars on eSafety and useful websites have been included in Appendix 4 on Page 17.

14. Bullying and Cyberbullying

Staff should be aware that students may be subject to cyberbullying via electronic methods of communication both in and out of school. Cyberbullying can take many different forms including:

- Email - nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms - potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites - typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming - abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones - examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information - may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyberbullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and students are reminded that cyberbullying can constitute a criminal offence. Students are encouraged to report incidents of cyberbullying to the College and, if appropriate, to the PSNI to ensure the matter is properly addressed and the behaviour ceases.

While there is no specific legislation for cyberbullying, the following may cover different elements of cyberbullying behaviour:

- Protection from Harassment (NI) Order 1997 - http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988 - http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003 - http://www.legislation.gov.uk/ukpga/2003/21

15. Communication of the College's eSafety and Digital Technology Policy

The College's eSafety and Digital Technology Policy is available for all users on the College's website: www.knock.co.uk and on Private Folders 1 for staff. All users are informed that the C2k Education Network is monitored and that security reports can be accessed by the ICT Coordinator and the Principal. Students and parents are encouraged to contact the Vice Principal (Pastoral Care) at any time to express their views on this policy.

16. How to Raise a Concern or Make a Complaint about the Administration of this Policy

If you have a concern or complaint about the administration of this policy, please contact Ms McCarthy, Vice Principal, in the first instance. If necessary, you may then access and follow the College's Parental Complaints Procedure which is available on the College website at www.knock.co.uk. Should you remain dissatisfied with the College's response after completing the internal complaints procedure, you can bring your complaint to the Northern Ireland Public Services Ombudsman within six months. Contact details for the Northern Ireland Public Services Ombudsman are provided on Page 11 of the Parental Complaints Procedure.

Signed: ***Mr Leo O'Reilly*** **Date: 6th June 2019**
(Chairperson of Board of Governors)

Signed: ***Miss Deborah McLaughlin*** **Date: 6th June 2019**
(Principal)

Appendix 1

Our Lady and St Patrick's College, Knock

Acceptable Use of Digital Technology - Staff

Digital Technology is to be used in a manner consistent with College Policies and in pursuit of the Aims of the College for the personal and educational development of the staff and students. Access to these facilities is a privilege, not a right.

1. Monitoring

The College has the right to access user data, including cloud services and mailboxes. Files stored within the College's network environment on servers, computers and devices will not be regarded as private and the College reserves the right (or C2k at the College's request) to monitor, review and examine the Internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on school laptops, servers, network devices and email systems, which it considers inappropriate, and prohibit the use of such material.

There is automatic filtering of all C2k mail for unsuitable content and for size. Mail, which is blocked, may be viewed by members of the Senior Leadership Team (Vice Principal (Pastoral Care) and Deputy Designated Teacher) who can then make a decision whether to allow the mail through the system and/or whether to take appropriate action within the terms of this eSafety and Digital Technology Policy.

The College maintains the right to examine staff usage of College Digital Technology and inspect any data recorded.

2. General Responsibilities

2.1 The College makes Digital Technology available to staff for use in carrying out official duties.

2.2 The decision as to which members of staff are provided with Digital Technology is at the discretion of the College.

2.3 During school hours, staff should only access websites which are directly linked to their school work.

2.4 Staff monitor student use of all Digital Technology and implement current College policies with regard to their misuse:

- 2.4.1 They report any suspected online misuse or a breach in eSafety to the Head of Year or the IT Manager as appropriate;
- 2.4.2 They report child protection concerns to the Designated Teacher for Child Protection;
- 2.4.3 eSafety issues are taught as per relevant schemes of work;
- 2.4.4 They are aware of eSafety issues related to the use of Digital Technology.

2.5 Staff must conduct themselves responsibly and honestly when using Digital Technology. They must ensure that their actions do not:

- 2.5.1 breach any law or statute, including data protection/GDPR guidelines; or otherwise bring the College into disrepute;
- 2.5.2 waste time or resources;
- 2.5.3 cause offence to colleagues or others.

2.6 Staff must not intentionally access, archive, store, distribute, edit, record, or reproduce any kind of inappropriate material on any of the College's Digital Technology.

2.7 Staff must view in advance any digital content, especially online content, to be used with students to ensure it is appropriate. Online videos must only be viewed full screen and with autoplay disabled.

2.8 All email communication with the wider school community must take place using official College accounts.

2.9 Digital devices may not be used for unauthorised commercial purposes.

2.10 Staff should understand the importance of adopting good eSafety practice when using Digital Technology outside school and realise that the College's eSafety and Digital Technology Policy covers their actions outside school, if related to their membership of the school or involving any member of the school community.

2.11 Staff must ensure they adhere to The Copyright, Designs and Patents Act.

3. Security

3.1 Staff must keep all passwords and user IDs confidential. The sharing of user IDs or passwords is prohibited at all levels. Users should ensure that strong passwords are used and stored securely.

3.2 Staff should log off or 'lock' a digital device, if leaving unattended, to prevent unauthorised use of their accounts.

3.3 It is the responsibility of users to ensure that confidential information (including photographs of students) is collected, stored and shared in compliance with General Data Protection Regulations.

4. Software

4.1 Staff must only acquire software with a direct educational use and have obtained permission from the IT Manager (who can check licencing issues).

5. Mobile Devices

5.1 The use of mobile devices for personal reasons should be restricted to Resource Areas, the staffroom, offices and preparation rooms. Mobile devices should not be used for personal reasons in the presence of students.

5.2 All staff are expected to comply with the following rules regarding the use of mobile phones in school:

5.2.1 Staff should not make or answer calls or texts while teaching a class or while doing any kind of supervisory duty. If a member of staff receives an emergency call while in class, he/she should step into the corridor or adjacent resource room, leaving the classroom door open and should end the call as promptly as possible.

5.2.2 Staff should not access social networking sites on mobile devices during class time or while doing a supervisory duty.

5.3 Staff provided with mobile devices for official business while away from College official premises, must take the necessary security precautions to avoid damage or loss.

5.4 Staff must not leave College digital devices in a car or in a place where they would be visible to thieves. If College digital devices are used at home, they must be stored securely.

5.5 Staff must not remove College digital technology without written approval from their line manager. Members of staff who have such approval must complete and sign a form, available from the IT Manager.

6. Social Networking

Individual members of staff who wish to use a social networking site (e.g. Twitter or Facebook) for school purposes must first request permission from the Principal. If permission is granted, they must adhere to the College's Code of Conduct for All Staff and Volunteers.

7. Sanctions

Where it is believed that a member of staff has failed to comply with this eSafety and Digital Technology Policy, they will face the College's Disciplinary Procedure.

8. Code of Conduct for All Staff and Volunteers (*Child Protection/Safeguarding Policy*)

Adopted from DE Circular 2017/04 (24/04/17) - Safeguarding and Child Protection - A Guide for Schools

The following guidelines should be read in conjunction with the College's Code of Conduct for All Staff and Volunteers.

Objective, Scope and Principles: This Code of Conduct is designed to give clear guidance on the standards of behaviour all College staff and volunteers are expected to observe. College staff and volunteers are role models and are in a unique position of influence and trust; they must, therefore, adhere to behaviour that sets a good example to all students within the College. As a member of a school community, each person has an individual responsibility to maintain his/her reputation and the reputation of the College, whether inside or outside working hours.

Extracts from the College's *Child Protection/Safeguarding Policy:*

1.2 All staff and volunteers must demonstrate high standards of conduct in order to encourage our students to do the same.

1.3 All staff and volunteers must also avoid putting themselves at risk of allegations of abusive or unprofessional conduct.

1.4 Teachers should avoid teaching materials the choice of which might be misinterpreted and reflect upon the motives for the choice.

3.1 All staff and volunteers must declare any relationships that they may have with students outside of school; this may include mutual membership of social groups, tutoring or family connections. Staff and volunteers should not assume that the College is aware of any such connections.

3.2 Relationships with students must be professional at all times. Sexual relationships with students are not permitted and may lead to an abuse of trust and criminal conviction.

6.1 All staff and volunteers must not engage in conduct outside work which could seriously damage the reputation and standing of the College or the staff/volunteer's own reputation or the reputation of other members of the College community.

eSafety and Internet Use

7.1 Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Regard should be given to the College's eSafety and Digital Technology Policy at all times both inside and outside of work.

7.2 Staff and volunteers must not engage in inappropriate use of social network sites which may bring themselves, the College, school community or employer into disrepute. They should not correspond with students through personal social networking sites or add them as 'friends'. Staff and volunteers should ensure that they adopt suitably high security settings on any personal profiles they may have.

7.3 Staff should exercise caution in their use of all social media or any other web based presence that they may have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others. This may also include the use of dating websites where staff could encounter students either with their own profile or acting covertly.

7.4 Contact with students must be via school authorised mechanisms. At no time should personal telephone numbers, email addresses or communication routes via personal accounts on social media platforms be used to communicate with students. If contacted by a student by an inappropriate route, staff should report the contact to the Principal immediately.

7.5 Photographs/stills or video footage of students should only be taken using College equipment for purposes authorised by the College. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photograph must be retained and destroyed in accordance with the College's Records Management Policy and Disposal Schedules.

9. Limitations of Use

Our Lady and St Patrick's College, Knock makes no warranties of any kind, whether expressed or implied, for the service it is providing. The College will not be responsible for any damages, including the loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. The College specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Agreement

All permanent and temporary staff who have been granted the right to use the College's Digital Technology are required to confirm by signature their understanding, acceptance and willingness to adhere to the College's eSafety and Digital Technology Policy.

Appendix 2

Our Lady and St Patrick's College, Knock

Acceptable Use of Digital Technology - Students

Digital Technology is to be used in a manner consistent with College Policies and in pursuit of the Aims of the College for the personal and educational development of the staff and students. Access to these facilities is a privilege, not a right.

1. Monitoring

The College uses **Securus**, an eSafety suite of tools available to schools via the C2k Education Network, to safeguard children in their use of information systems and electronic communications. It monitors the screen display and keystrokes of students and triggers a capture if the content is listed in the database of inappropriate words and phrases

The College has the right to access students' data, including cloud services and mailboxes. Files stored within the College's network environment on servers, computers and devices will not be regarded as private and the College reserves the right (or C2k at the College's request) to monitor, review and examine the Internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on digital devices and email systems, which it considers inappropriate, and prohibit the use of such material.

There is automatic filtering of all C2k mail for unsuitable content and for size. Mail, which is blocked, may be viewed by members of the Senior Leadership Team (Vice Principal (Pastoral Care) and Deputy Designated Teacher) who can then make a decision whether to allow the mail through the system and/or whether to take appropriate action within the terms of this eSafety and Digital Technology Policy.

A student will be required to hand over his/her digital device and passcode to a member of staff if:

- there is a suspicion that the digital device has unsuitable material stored on it;
- a student has disrupted a lesson through improper use of a digital device;
- a student has misused his/her digital device, without staff permission, to take photographs/video;
- the digital device or any of its features has been used for any form of bullying;
- games are being played on the digital device during school hours;
- the digital device has been used to breach any school rule/policy and general well-being of staff and students.

2. Sanctions

If unsuitable material is found on any digital device, including cloud storage and email, it will be referred to the appropriate member of staff. Inappropriate use will result in access being withdrawn to digital services. Any student who refuses to cooperate or violates any aspect of this eSafety and Digital Technology Policy may face disciplinary action as deemed appropriate in keeping with the College's Positive Behaviour Policy.

3. Rules Governing Student Use of Digital Technology

1. Students are not permitted to use any digital devices in the College, except with the explicit permission of a member of staff.[2]
2. The DE funded C2k Education Network is the primary Internet provider. Students are only permitted to access the Internet using mobile data with the explicit permission of a member of staff.
3. Students may not log on using another person's username.
4. If unsuitable material is encountered by a student, he/she must inform the teacher/IT Manager immediately. Mr Ashe will refer the matter to the respective Head of Year, the Designated Teacher for Child Protection or the Principal, as appropriate. A student must never feel uncomfortable when viewing any resources on the computer networks.
5. At all times students must only access online content which is directly linked to their school work.
6. All users are expected to use the Internet to research topics consistent with the Aims of the College.
7. Students must not attempt to bypass filtering or to access inappropriate or illegal material.
8. Students must not execute any program received in email or found on a web page except as directed by the IT Manager or a teacher.
9. Students must not install or download any program/file except as directed by the IT Manager or a teacher.
10. Students must not engage in any illegal activity, use obscene or racist language or retrieve, send, copy or display offensive messages, pictures or videos.
11. Students must refrain from cyberbullying and adhere to College's Anti-Bullying and Positive Behaviour Policies.
12. Students must not post any content online or record any media which would bring discredit on the College.
13. Digital devices (with the exception of mobile phones) brought into school must only contain work files and no software programs or games. Digital devices containing programs or games may be confiscated. All portable storage devices should be regularly virus scanned.
14. Digital devices must not be used for unauthorised commercial purposes on College premises.
15. Students must not attempt to break passwords of other students or staff, or access any digital device apart from their own.
16. Students must not intentionally damage or modify any digital technology or use any software that can damage or override security.
17. Students are not permitted access to the server or hub rooms.
18. Students must adopt good eSafety practice when using Digital Technology outside school and realise that the College's eSafety and Digital Technology Policy covers their actions outside school, if related to their membership of the school or involving any member of the school community.
19. Students must adhere to The Copyright, Designs and Patents Act.

4. Limitations of Use

Our Lady and St Patrick's College, Knock makes no warranties of any kind, whether expressed or implied, for the service it is providing. The College will not be responsible for any damages, including the loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. The College specifically denies any responsibility for the accuracy or quality of information obtained through its services.

[2] For educational purposes only, Upper School students are permitted to use portable digital devices in the Sixth Form Study, Library or Common Room.

Internet Safety for Students and Parents

Inappropriate use of the Internet and mobile technologies, such as trolling, sexting, cyberbullying or sexual exploitation, can, as we are all aware, have a devastating impact on the lives of our children and young people. The following advice has been supplied by the Department of Education in collaboration with the PSNI and it is endorsed by the Safeguarding Board for Northern Ireland (SBNI).

General advice to everyone:

We all deserve to be able to use the Internet to learn, explore and connect with each other. But all of us need to be aware of the risks involved in doing so, especially on social media. Our advice is:

- Don't share personal information or images with people you don't know.
- Don't accept friend requests with someone you don't know – not everyone online may be who they say they are.
- Set privacy settings on all devices so that only people you know can view your account.
- Don't post anything online that you are not happy to be shared, particularly nude or nearly nude images or videos. It may seem like a bit of fun with friends at the time but there is always a chance those images could be shared or get into the wrong hands and could lead to harmful situations such as stalking, abuse or blackmail.
- If someone has made you feel uncomfortable or you have had disturbing interaction online, tell police or a trusted adult. You can ring the police on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.
- The Internet can be a great place but it is important to remember there are people out there who may wish to abuse, exploit, intimidate or bully you online – if this happens to you, tell someone immediately.
- Remember that if things do go wrong online, there are people who can help.
- If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further such incidents. You will not get into trouble.

General advice to parents:

- The most important thing is to have conversations with your children - talk to them about the benefits and dangers of the Internet so that you can empower them to use the Internet safely.
- Cultivate an interest in their online activities - their favourite websites, online games and interests and keep an eye on what they are doing online.
- Don't be afraid to ask your children who they are talking to online and what they are talking about and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried because there are people who can help.
- Become a 'net-savvy' parent - the best safeguard against online dangers is being informed. Jump in and learn the basics of the Internet - read articles, take a class, and talk to other parents. You don't have to be an expert to have a handle on your child's online world.
- Go to www.getsafeonline.org for lots of useful advice and information on how to stay safe online. Safeguardingni.org will also provide information for parents and carers on e-safety.
- Links to other sites that can provide information and advice to young people and parents are available from the DE website at: http://www.deni.gov.uk/index/pupils-and-parents/pupils.htm

Appendix 4

eSafety: DE Circulars, Guidance and Related Documents

DE Circular 2007/01 (18/06/07) - Acceptable Use of the Internet and Digital Technologies in Schools

DE Circular 2011/22 (27/09/11) - Internet Safety

DE Circular 2013/25 (06/12/13) - eSafety Guidance

DE Letter (12/06/15) - General Advice to Everyone/General Advice to Parents

DE Circular 2016/26 (01/12/16) - Effective Educational Uses of Mobile Digital Devices

DE Circular 2016/27 (01/12/16) - Online Safety

C2K Information Sheet ENO74 – Acceptable Use Policy for C2k Services

Useful Websites

- www.deni.gov.uk/index/pupils-and-parents/pupils.htm
- www.thinkuknow.co.uk
- www.childnet.com
- www.getsafeonline.org
- www.safenetwork.org.uk
- www.saferinternet.org.uk
- www.ceop.police.uk
- **Safeguarding Board for NI**
  www.safeguardingni.org
- **Childline** 0800 1111
  www.childline.org.uk
- **NSPCC** 0808 800 5000
  www.nspcc.org.uk