WELLINGTON COLLEGE BELFAST

E-Safety and Acceptable Use of ICT Policy

Context

Learning and teaching is facilitated, developed and strengthened by the effective use of information and communication technology. To prevent harm and misuse, this policy provides a framework within which e-learning can be implemented safely.
It acknowledges and complies with DE Circulars 1999/25, 2007/01, 2011/22, 2013/25, 2016/26 and 2016/27.

Rationale

Wellington College recognises that ICT and the internet are effective tools for learning and communication that can be used in College to enhance the curriculum, challenge students, support creativity and develop independence. Using ICT can be beneficial, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good e-safety. It is important that all members of the College community are aware of the dangers of using the internet and know how they should conduct themselves online.
The internet is used in College to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the College's management functions. Technology is advancing rapidly and is now a significant part of everyday life, education and business.

Policy Aims

The aims of this policy are to:

- Support students and staff in the positive use of digital technologies
- Ensure the safety of all students and staff in relation to digital technologies and online activities both in and out of College
- Help students recognize inappropriate activities and situations and respond in a safe manner in such circumstances
- Prevent the misuse of digital technologies, and where it occurs to respond within the parameters of the Code of Behaviour
- Protect staff, students and parents from erroneous or malicious allegations
- Meet legal obligations in relation to child protection matters The policy should be read in conjunction with other relevant policies. It will be reviewed on a regular basis.

ICT Facilities in Wellington College

Wellington College has a large number of computers, printers and scanners in every part of the College. Students are encouraged to make use of the network for all aspects of their work. Filtered internet access is available at every station and all students have a secure email account. This is the only email account that students may use in College.
Before a student can use the network, send a College email or access any internet site it is important that they and their parents have read and fully understand these terms and conditions of use and the relevant parental consent has been provided (see Appendix 2).
The network is a learning and teaching tool to support College studies. It is not a recreational medium and should not be used as such.

Usernames and Passwords

The College is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of College data and personal protection of the College community very seriously.

To access the College network each student has a unique username and password. Students should remember their username and password and keep these secure at all times. It is not a good idea to write passwords down. All students will be held accountable for the data that is stored in their network area and for activities that are carried out in their name. The ICT Technician may be contacted if students have enquiries about passwords. Students should bear in mind that C2K systems policies dictate that passwords are changed every 120 days; however, if a student feels that his/her password has been compromised it can be changed by holding down Ctrl, Alt and Delete and choosing 'Change A Password', or by contacting IT Support.

Data Storage and Transfer

It is recognised that both staff and students will continue their work at home and they can transfer or access their data in a number of ways:

- By saving work on to a USB memory stick. Students should write their names on memory sticks if possible, otherwise re-name the device using their own name. For documents containing personal data, staff must either password protect the USB memory stick using 'Bitlocker', or password protect any documents or files containing personal data;
- By email attachment although this will be subject to filtering;
- By logging on directly to their 'C2K Documents' from home.
- By using the College approved VLE (Google Classroom).
- Work should be saved in at least 2 places for backup purposes.

Bring Your Own Device Policy

The Bring Your Own Device Policy outlines the terms of use for sixth form students who may wish to bring their own device to study in College.

Email

C2k issues every member of staff and student with an email address.
Staff should be aware of the following regarding the use of College email:

- Use official College-provided email accounts only to communicate with students or parents/guardians. SchoolComms is the preferred system to do this. Personal email accounts should not be used to contact parents or students;
- Send professionally and carefully written emails from College accounts;
- Inform the relevant line manager or a member of the Senior Leadership Team if offensive, threatening or unsuitable emails are received, either from within the College or from an external account. Staff should not attempt to deal with this themselves. Students should be aware of the following regarding the use of College email:
- Use College-approved email accounts only (with the exception of UCAS applications);
- Social emailing will be restricted;
- Inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the College or from an external account. Students should not attempt to
  deal with this themselves;
- Be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
  Students will be educated on the use of email and the associated risks through the ICT curriculum and the preventative curriculum.

E-Safety and the Curriculum

The importance of e-safety is emphasised across the curriculum and students are educated in the benefits and dangers of the internet and how to use it in a safe and productive way. Students are all made fully aware of the College's code of conduct regarding the use of ICT and technologies and behaviour online.
In lessons where internet usage is planned, students will be guided to suitable sites; where students are permitted to freely search the internet, staff will be vigilant and monitor the content of websites students search.
E-safety and appropriate internet usage messages are delivered through Year 8 ICT classes, through the Personal Development programme, through assemblies and by external speakers such as the PSNI.

Social Media

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught, as part of the preventative curriculum, about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. Online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that students are educated so that they can make their own informed decisions and take responsibility for their conduct online. Students should take great care with the opinions which they express and content which they include on social media. The College takes no responsibility for items that are uploaded to such sites by students out of College hours and out of College. However, the College will take appropriate action against any member of the College community who brings the College into disrepute on a website or app which can be viewed publicly.
All members of the College community, including parents, are asked to be sensitive to the privacy of others and to report any abuse or any potential case of cyber-bullying. Cyberbullying, as with any other form of bullying, is taken very seriously by the College. Information about specific strategies in place to prevent and tackle bullying are set out in the Anti-Bullying Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do things that they otherwise would not do in person. It is made very clear to members of the College community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. The Anti-Bullying Policy is available on the College website.

All reputable websites have a section for reporting abuse. The College's website contains a link on the home page to the CEOP Internet Safety website with information on staying safe online.

Risks associated with Internet Access.

The worldwide nature of the internet means that it is not possible for any government or organisation to have any control of it.

In common with other media such as magazines, books and videos, it is a reality that material exists on the internet which most people would find offensive. The only way of completely blocking access to this kind of material is to restrict the range of pages available, in which case the global and dynamic nature of the internet will be lost. Parents should be aware of these dangers. Students should realise that if they reach an unsuitable site, it may be closed at an early stage before they are offended. Any undesirable material which escapes the filtering system should be reported to a member of teaching staff.

C2k and the College work together to provide filtered access to the internet. This means that searches for certain keywords will be denied as will access to particular sites. This filtering extends to the system 'reading' the content of pages accessed, and determining whether the information contained is appropriate for use in College. The filtering system in use records each and every website visited along with anything that has been requested.

Google Classroom

All Wellington College students have access to Google Classroom. All information, including pictures, stored on Google Classroom are secured by password. The use of Google Classroom greatly enhances the opportunities for 'anytime', 'anywhere' learning in a structured and independent way. Google Classroom can contain course information, online content, communication tools, online submission of work and subsequent feedback, tracking facilities, links and much more.

Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The College will risk-assess any new technologies before they are allowed in College, and will consider any educational benefits that they might have. The College keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Using the Network

Students are responsible for good behaviour whilst using the network and general College rules apply. This must be borne in mind, especially when students communicate with one another using e-mail and in College chatrooms or discussion boards.

The network (including the internet) is provided in support of learning and all users are responsible for their behaviour and communications over the network. It is assumed that users will comply with College standards and will honour the agreements they have signed.

The College has a legacy network managed by the College in addition to the C2K network.

The College may examine files held on its computer system and all internet traffic, including e- mail, will be monitored. In the event of unsuitable material being found, the College may take whatever action it deems appropriate. There should be no expectation of privacy for users of the network.

Access to, as well as within, the network and internet is configured according to individual privileges. All potential users of the network and their parents are asked to read the terms of use outlined on the following pages.

Terms of Use
The following are not permitted:

- Eating or drinking at a computer;
- Using any software not registered with the College, including downloads;
- Changing settings on any computer;
- Adding or removing items of hardware without permission;
- Sending or displaying offensive messages or pictures;
- Using offensive or obscene language;
- Activity which threatens the integrity of the College computer system, or activity which
  attacks or corrupts other systems;

- Activities which are not relevant to the College curriculum;
- Violating copyright laws including downloading, saving or sharing music/video files;
- Accessing the network using any password except your own;
- Disclosing your password to anyone else;
- Trespassing in others' folders, work or files;
- Use of the network or any College computer to access and/or download inappropriate

material on the internet;

All e-mails that are trapped by the filtering software may be read by the system's administrators before they are released.

Violations of any of the rules above may result in temporary or permanent exclusion from the network or the withdrawal of equipment on loan.

Parents will usually be informed in writing if an exclusion takes place and may be asked to request reinstatement.

Parents may also be invited into College to discuss the problem and in extreme cases will be supplied with copies of the offensive materials.

Securus

- Securus is an e-monitoring application that monitors students/guest users on c2k managed devices using keystroke monitoring and application monitoring technologies
- Through this application issues such as cyber bullying, online grooming/child abuse, self-harm and suicidal ideation, racial/homophobic/religious harassment, use of drugs/weapons, attempts to use a proxy bypass can be detected
- Alerts specified staff to potential child protection issues and encourages students to use technology responsibly
- Staff, students and parents will be informed

Protecting Personal Data

The College takes the protection of personal data very seriously and believes that protecting the privacy of staff and students and regulating their safety through data management, control and evaluation is vital to College and individual progress. The College collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student progress, and strengthen pastoral provision. The College takes responsibility for ensuring that any data that is collected and processed is used correctly and only as is necessary. Policies and procedures are compliant with the General Data Protection Regulations 2018.

Using Student Image and Work

Images of students and student work will not be displayed in public, either in print or online, without consent. On admission to the College parents/carers will be asked to sign a consent form. Parent / carers may withdraw consent at any time.
Staff should ensure that any images of students stored digitally should be stored on the C2k network. Staff must transfer digital media from capture devices to the C2k network at the earliest possible opportunity; it is expected that digital images of students should be deleted from portable devices as soon as possible. It should not be normal practice to store images of students on digital media devices, in a printed format or on any external memory device, for any longer than is necessary.

E-Safety Responsibilities of Staff

• read and promote the College's E-Safety and ICT Acceptable Use Policy;
• be familiar with the suite of pastoral policies including Safeguarding and Child Protection, Positive Behaviour, Anti Bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately;
• ensure they know what to advise a child who reports a concern relating to any communication or material he/she has received online;
• be responsible for ensuring the safety of personal and confidential College data and information: USB sticks should be encrypted/files containing sensitive or personal data should be password protected;
• observe students carefully when using technology or conducting online searches;
• remind students that their use of the internet is monitored and that they should not share usernames and passwords;
• maintain a professional level of conduct in their use of technology;
• report all e-safety incidents to a member of the Designated Team.

E-Safety Responsibilities of Students

• read and adhere to the E-Safety and ICT Acceptable Use Policy and follow all safe practice guidance;
• develop an understanding of the risks posed by the use of technology and take responsibility for their own use of technology both inside and outside College;
• be responsible for ensuring the safety of personal information: USB sticks should be encrypted / files containing sensitive or personal data should be password protected;
• avoid sharing their password with any other person;
• show respect to others in their use of technology both in College and at home;
• develop and understanding of what they should do if they feel uncomfortable or at risk when
using technology;
• discuss e-safety with family and friends;
• report any e-safety concerns to a member of staff.

E-Safety Responsibilities of Parents

• read the E-Safety and ICT Acceptable Use Policy with their children;
• help and support the College in promoting e-Safety;
• develop an understanding of e-Safety risks and an awareness of the guidance available to support students and parents;
• contact the College if they have any concerns regarding their child's safety.

E-Safety Advice for Students

1. Do not give out any personal information e.g. phone number, address etc.
2. Do not open any messages from people you do not know.
3. Do not become friends with someone you do not know.
4. Never arrange to meet someone who you have only met online. Not everyone you meet online is who they say they are.
5. If something you have read or seen online causes you concern talk about it with a responsible adult who will advise you how to deal with it.
6. Think very carefully before posting any pictures of yourself online. The picture will no longer be in your control and it can be downloaded or screenshot.
7. Do not post images of other people without their consent. You might think posting a funny
picture will cause no harm but it might cause someone real distress and hurt their feelings.
8. Do not share your password with other people.
9. Keep your privacy settings as high as possible.
10. Think carefully before making any posts online. Respect other people's views. Even if you
don't agree with what they say, you do not need to be rude.

E-Safety Advice for Parents

1. Talk to your child about the benefits and risks of internet use so that you can help educate them to use the internet safely.
2. Develop an interest in your child's online activities, including favourite websites, online games and interests, and be aware of what your child is doing online.
3. Be aware of your child's use of social media.
4. Ask your child who he/she is talking to online and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried.
5. Be aware of the advice and information available relating to e-safety. Websites containing advice for parents and children include:
www.ceop.police.uk
www.childline.org.uk
www.nspcc.org.uk
www.net-aware.org.uk/#
www.getsafeonline.org
www.thinkuknow.co.uk
www.internetmatters.org
www.saferinternet.org.uk

https://www.vodafone.com/content/digital-parenting.html/#

Appendix 1 – Procedure for responding to a sexting incident

Definition of 'sexting'
For the purposes of this advice sexting is simply defined as: 'Sending or posting of sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the internet.'

Students need to be aware that it is illegal, under the Sexual Offences (NI) Order 2008, to take, possess or share indecent images of anyone under 18. Additionally, if a student is affected by inappropriate images or links on the internet, they need to be made aware that they do not forward the image or link to anyone else. These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.

We recognise there are many different types of sexting and it is likely that no two cases will be the same. We realise the importance of carefully considering each case on its own merit and applying a consistent approach to help protect students, staff and the College.

1. What to do if a child makes a disclosure about a sexting, or suspected sexting incident:
Whatever the nature of the incident, ensure College safeguarding and child protection policies and practices are adhered to. (Safeguarding and Child Protection Policy)
- Act Promptly
- Do not investigate yourself
- Contact the designated teacher
- Report your concerns and make full notes.

2. If indecent images of a child are found, staff should:
- Report the incident to the Designated Child Protection Teacher
- The Designated teacher should assess the risk to the child or young person and make referrals as appropriate, taking advice from the Child Protection Team at EA if necessary. If the image has been shared on the College network, social network or website the College will:
- Block the network to all users and isolate the image.
- Images should not be moved, sent or printed.

3. Deciding on a response:
- It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a College it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.
- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make contact with parents to inform them of the issues (where appropriate)

• Make a Social Services referral if needed
• Contact the police (if appropriate)
• Put the necessary safeguards in place for the student, e.g. they may need counselling support, immediate protection and parents must also be informed.

4. Care provided after the incident:
The College will support the emotional and social well-being of the child / children who have been involved through:
• Monitor and support their return to College
• Refer to outside agencies where appropriate e.g. Barnardo's 'Safer Choices Programme'.
• Offering access to a counselling service (where appropriate)
Information for Students on the risks associated with social networking sites including advice on how to avoid the risks and enjoy using these sites. Quick tips on how to protect your mobile devices. Detailed information on how to protect your mobile devices. Information on the sexting, protecting yourself, the law. How to stay in control and what to do if an image falls into the wrong hands

http://www.connectsafely.org/wp-content/uploads/snapchat_guide.pdf

Appendix 2 – Acceptable Use Policy Agreement

WELLINGTON COLLEGE BELFAST
Co-educational Grammar School

INTERNET ACCEPTABLE USE POLICY

Agreement to Comply ***Parent AND Student - Please sign page 4 of the pupil information form and retain this sheet for your information.***

Student: I understand and will abide by the Wellington College Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offence. Should I commit any violation:

1. my access privileges may be revoked and
2. school disciplinary action and/or appropriate legal action may be taken.

I understand and accept that:

- Use of the College's Internet account is a privilege, not a right;
- The Internet is to be used for educational and research purposes only, consistent with the educational aims of the College;
- Misuse will result in loss of my right to access the Internet through school computers;
- Wellington College will monitor pupil use of the Internet, including e-mail, to determine that use is for the stated purposes. For this and other reasons, e-mail is not private. Violations that may lead to revocation of Internet access include:
  - playing computer-based games;
  - downloading excessively large files;
  - sharing passwords with anyone besides Wellington College Staff;
  - subscribing to inappropriate newsgroups;
  - E-mail correspondence inappropriate to educational purposes;
  - any activity posing potential risks to myself or others;
  - harassing other users (e.g. with unwanted e-mail messages or inappropriate content on social networking sites;
  - illegal activity;
  - revealing mine or another's home address/phone number;
  - vandalism of accounts or systems;
  - using abusive, vulgar, or other inappropriate language or forms of cyber-bullying;
  - failure to report known security problems;
  - any other inappropriate use or misuse of the facility;
  - accessing sites of an inappropriate nature;
  - misuse of WEB technologies.

Wellington College Staff will deem what is inappropriate use, and their decision is final. Accounts are monitored and use of the account signifies agreement to such monitoring. Wellington College Staff may close an account at any time for violations.

Links to other policies
This policy should be read in conjunction with the Mobile Phone Policy and the E-Safety Policy.
Student to sign page 4 of the pupil information form.

Parent or Guardian: As the parent or guardian of this student, I have read the Internet Use Agreement. I understand that this access is designed for educational purposes. I recognise that it is impossible to limit all misuse and staff cannot control all student activity, and I will not hold Wellington College responsible for any improper or illegal use of the Internet in school by my child. Further, I accept full responsibility for supervision if and when my child's use of the College system or software is not in a school setting. I hereby give permission to permit Internet access for my child and certify that the information contained on this form is correct.
Parent to sign page 4 of the pupil information form.

Appendix 3 – C2K Agreement Covering the Loan of Equipment

TERMS AND CONDITIONS COVERING THE LOAN OF THE IT EQUIPMENT

The Education Authority (EA) has agreed with the School that that the identified IT Equipment as detailed in the attached IT Equipment Loan Record will be loaned by it to you for the educational benefit of your child for a period initially up to date listed on cover page. This loan is subject to review on a regular basis, and can be withdrawn by EA at any time. EA also reserves the right the substitute the IT Equipment at any time if necessary.

As a parent/guardian/carer of a pupil and the Responsible Person to whom IT Equipment has been loaned you have read and agreed to the following terms and conditions:

1. The IT Equipment remains the property of EA and has been loaned for the sole purpose of assisting in the delivery of the school curriculum to the Named Pupil or pupils.
2. When the term of this Agreement ends you as the Responsible Person will return the IT Equipment to the School Contact by a specified time and in a specified manner.
3. You should return the IT Equipment to the School Contact in the same condition as you received it excepting for reasonable wear and tear.
4. You should return the IT equipment in person so that it can be inspected by the School for any visible damage.
5. Any change of home address by the Named Pupil must be notified to the School Contact without delay.
6. The IT Equipment and the connectivity equipment must not be used for any illegal and/or anti-social purpose.
7. The IT Equipment may be used by other family members whilst supporting the named Pupil's education but must not be used for any other activities unless otherwise approved by the School. On no account must the IT Equipment be used by anyone else or be allowed to go out of the possession of the Responsible Person or Named Pupil.
8. As the Responsible Person you must ensure that:
    a. The Named Pupil and any permitted family user supporting the named Pupil's education treats the IT Equipment with appropriate care and the IT Equipment is maintained in good condition.
    b. The IT Equipment is not left unattended without being stored securely.
    c. The Named Pupil and any permitted family user avoids food and drink near the IT Equipment.
9. Neither EA nor the School can accept responsibility for the loss of work in the event of the IT Equipment malfunctioning.
10. It is the responsibility of the Named Pupil to back-up their work regularly.
11. You must only use software licensed, authorised or installed by the School or by EA through C2k.
12. Anti-Virus software installed by the School or EA through C2k must not be uninstalled.
13. There may be occasions when either EA or the School will need the IT Equipment to be returned to the School /EA for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the IT Equipment. Neither EA nor the School can be held responsible for

the loss or damage of any data on the IT Equipment during this process. The IT Equipment must be returned to the School without unnecessary delay by the Responsible Person as and when requested.

14. During the upgrade and maintenance process, technical members of School or EA staff may view data or programmes on the IT Equipment. You will be held responsible for ensuring use of the IT Equipment is in accordance with the School's acceptable use policy at this point. You may want to remove personal data from the IT Equipment before its return.
15. All technical support and maintenance issues must be raised with the School Contact initially without unnecessary delay.
16. If the IT Equipment is stolen you must immediately report it to the police and get a crime reference number. You must immediately report this to the School Contact.
17. If the IT Equipment is accidentally damaged, you must immediately contact the School Contact and the equipment presented for examination. You must not arrange to have repairs undertaken elsewhere. The School /EA will do its best to repair the damage. If this is not possible, replacement will be considered on a case by case basis. If this damage is not the result of normal wear and tear, you will be liable to reimburse EA for any reasonable repairs and labour costs.
18. As the Responsible Person you must ensure that that the external face of the equipment provided is not decorated or changed in any way, including affixing stickers.
19. Reasonable health and safety precautions should be taken when using the IT Equipment. Neither EA nor the School is responsible or any damage to person or property resulting from the IT Equipment loaned.
20. Neither EA nor the School is responsible for any costs resulting from the use of the IT Equipment and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.
21. Neither EA nor the School is responsible for any broadband charges incurred by the Named Pupil or any permitted family user of the IT Equipment accessing the internet from any site other than school premises are not chargeable to the school.
22. You will ensure that any internet access using of the IT Equipment at home is for an appropriate educational purpose.
23. All information and supporting documentation supplied by you with this Agreement will be used for the sole purpose of providing the IT equipment. Your IT Loan Agreement and related information, will be held and maintained by the School in accordance with the provisions of Data Protection Legislation. The data will not be passed to any other third party without your consent, except when the School is required to do so by law.
24. By accepting the IT Equipment you are confirming that you have read and agree to adhere to current School policies regarding the following: Acceptable Use, Data Protection, Computer Misuse and Health and Safety which are attached to this Agreement.

Both EA and the School reserve the right not to replace a lost or damaged device.

Responsible Person (Parent/Guardian/Carer) Agreement:

I have read and agree to be bound by the terms and conditions set out above.
Name of Responsible Person (parent / Guardian / Carer):……

Signature parent/ Guardian / Carer: ……

Date: ……..