# Wellington College Belfast

# E-Safety Policy

Reviewed by Board of Governors November 2016

# Wellington College Belfast
# E-Safety Policy

## Policy

It is College policy to provide a safe and secure digital learning environment for pupils and staff and to improve their skill level

## Policy Aims

The aims of this policy are to:

- Support pupils and staff in the positive use of digital technologies
- Ensure the safety of all pupils and staff in relation to digital technologies and online activities both in and out of school
- Help pupils 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.

**DENI circular 2013/25** defines **E-Safety** as short for 'electronic safety'.

## Roles and Responsibilities

Principal

The Principal has a duty of care for ensuring the safety (including E-safety) of all members of the school community, though the day to day responsibility for E-safety is delegated to the *ICT Co-ordinator*.

The Principal and the Designated Teacher for Child Protection should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

ICT Co-ordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College's e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
- provides training and advice for staff
- liaises with C2k
- liaises with school technical staff

Teachers and support staff

are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current College E-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)

- they report any suspected misuse or problem to the Principal
- all digital communications with pupils/parents/carers are on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- appropriate websites only are accessed in the College for educational purposes

The Designated Teacher for Child Protection

should be trained in E-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

are responsible for using the College's technology systems in accordance with the Pupil Acceptable Use Policy.

- They should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They need to understand the importance of reporting the abuse of any hardware
- They need to report accessibility to inappropriate websites in the College
- They will be expected to know and understand policies on the use of mobile devices and digital cameras
- They should also know and understand policies on the taking/use of images and on cyber-bullying
- They should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the College's E-Safety Policy covers their actions out of school, if related to their membership of the school
- They should never reveal personal details about themselves or others in any digital format

Parents/Guardians

play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The College will take every opportunity to help parents understand these issues through Parents' Evenings, email, letters, website and information about national/local E-safety campaigns/literature. Parents and carers will be encouraged to support the College in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the College

## Professional Development for Teachers

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

- *A planned programme of formal E-safety training will be made available to staff at the beginning of each academic year. This will be regularly updated and reinforced. An audit of E-safety training needs of staff will be carried out.*
- *All new staff should receive E-safety training as part of their induction programme, to ensure they understand the school E-safety policy and Acceptable Use Agreements.*
- *The ICT co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff/departmental meetings/training days.*
- *The ICT co-ordinator will provide advice/guidance/training to individuals as required*

## Education of Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the College's E-safety provision. Pupils need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

Staff should reinforce E-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety curriculum will be provided as part of ICT/PSE classes and will be regularly revisited
- Key E-safety messages will be reinforced as part of a planned programme of assemblies (e.g. Safe Internet Day) and form period activities
- Pupils will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge sources and to respect copyright
- Pupils will be instructed in the need for a Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Technician temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Risk assessments

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become “Web-wise” and ultimately good “digital citizens”. Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school’s Acceptable Use Policy. (DENI 13/25)

### Cyberbullying

Bullying, intimidation and harassment are not new; however bullying via electronic media both in and out of school represents a new challenge for schools to manage.

Staff should be aware that pupils may be subject to cyber bullying via electronic media both in and out of school. This form of bullying should be considered within the College’s overall Anti-bullying Policy and pastoral services as well as the E-Safety policy.

Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.

Cyber Bullying can take many different forms and guises 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. (DENI 15/25)

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying 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

It is important that pupils report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Staff should also keep good records of cyber-bullying incidents, following the College's Anti-Bullying Policy to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions. (DENI)

## Dealing with breaches of the Guidelines

Misuse of mobile phones will be dealt with using the same principles set out in the Code of Behaviour, with the response being proportionate to the severity of the misuse. The VPP will deal with serious incidents of misuse, particularly where there has been a victim of cyberbullying.

Pupils should be aware that serious misuse may lead to the confiscation of their mobile phone, communication with parents and the imposition of other sanctions up to and including exclusion from school. If the offence is criminal in nature it will be reported to the PSNI.

Where it is deemed necessary to examine the contents of a mobile phone this will be carried out by a designated member of staff. The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

## Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the school's Code of Behaviour resulting in sanctions being applied:

- Photographing or filming staff or other pupils without their knowledge or permission
- Photographing or filming in toilets, swimming pool and changing rooms and similar areas
- Bullying, harassing or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- Refusing to switch a phone off or handing over the phone at the request of a member of staff

Using a mobile phone outside school hours to intimidate or upset staff and pupils will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

## Sanctions

Pupils and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines following the Code of Behaviour policy. In addition pupils and their parents should be very clear that the school is within it rights to confiscate the phone where the guidelines have been breached.

If a phone is confiscated school will make it clear for how long this will be and the procedure to be followed for its return.

Pupils should be aware that the PSNI will be informed if there is a serious misuse of a mobile phone where criminal activity is suspected

If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff the ultimate sanction may be permanent exclusion. The College will consider the impact on the victim of the act in deciding the sanction and parents will be involved.

## Where the phone has been used for an unacceptable purpose

The Principal or a designated staff member will have the right to view files stored in confiscated equipment and will seek the cooperation of parents in deleting any files which are in clear breach of these Guidelines unless these are being preserved as evidence.

If required evidence of the offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.

Advice can be sought from the EA B Child Protection Team and/or the PSNI. The school will also consider whether an incident should be reported to the school Designated Teacher.
The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation in line with the school's Anti-Bullying Policy.

## Communication of the E-Safety Policy

Communication with pupils

- All users will be informed that C2k network and Internet use will be monitored
- An E–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils
- An E–Safety module will be included in the pastoral and ICT programmes covering both safe school and home use
- E–Safety training will be part of the transition programme across the Key Stages
- E-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable
- Pupils must never

Communication with staff
It is important that all staff feel confident to use new technologies in teaching and the College's E–Safety Policy will only be effective if all staff subscribe to its values and methods.

- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the College will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the SMT and have clear procedures for reporting issues.
- The College will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.

## Email security

In the school context emails should not be considered private. C2k recommend that all staff and pupils should be encouraged to use their C2k email system. It is strongly advised that staff should not use home 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.

### C2k Internet security

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution.
Access to the Internet via the C2k Education Network is fully auditable and reports are available to the principal.

### Legacy Internet Security

Censornet.com is the internet filtering provider used throughout all computers on our legacy network.

http://www.censornet.com/education/secure-web-gateway/

- The solution protects against malware, time wasting, illegal or inappropriate content and provides a complete audit trail of web activity for peace of mind and accountability
- It prevents accidental or intentional access to malware, inappropriate and illegal web-based content using the latest real-time scanning technology from BitDefender.
- Reduces legal risk exposure **–** blocks known illegal content, inappropriate images and web content and creates an audit trail of activity for every user on the network should evidence be required.

Essentially no one in the College (staff included) is able to access the Internet on the legacy network without passing through this web filter. It enables the College to have complete safety against known problematic websites and allows the College to immediately block access to websites.

## Legal Framework

### Public Order (N.I.) Oder 1987

This Act makes it a criminal offence to stir up hatred or arouse fear. Fear and Hatred both mean fear/hatred of a group of persons defined by reference to religious belief, colour, race, sexual orientation, disability, nationality or ethic or national origins

### Criminal Justice (No2) (N.I.) Order 2004

Commonly referred to as N.I. ‘Hate Crime’ legislation. This empowers courts to impose tougher sentences when an offence is aggravated by hostility based on the victim’s actual or presumed religion, race, sexual orientation or disability.

### Protection of Children (N.I.) Order 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in Northern Ireland. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.

## Sexual Offences (N.I.) order 2008

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

## Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

## Protection from Harassment (N.I.) Order 1997

Article 3.This legislation can be considered where a person is pursuing a course of conduct which amounts to harassment. This includes alarming a person or causing a person distress. This course of conduct must be on more than one occasion

## Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner’s Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

## The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else’s password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

## Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

## Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programmes all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

## Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

## Criminal Justice and Immigration Act 2008

Sec 62-68 Includes the Coroners and Justice Act. It is an offence to possess a drawing or painting which depicts a child in an indecent pose or participating in an indecent act.

Section 63 offence to possess "extreme pornographic image"

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

## Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

• Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.

• School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti bullying policy.