Belfast Boys' Model School

E-Safety Policy

Created May 2022

This policy is to be used in conjunction with the following Belfast Boys' Model School policies:

- Acceptable Use Policy (Pupil)
- Acceptable Use Policy (Staff)
- Remote and Blended Learning Policy
- Anti-Bullying Policy
- Positive Behaviour and Discipline Policy

Devices covered by the policy include:

- Mobile phones
- Tablets (including IOS, Android & Windows-based devices)
- Lap tops, Surface Pros & multi-function devices, Chromebooks
- Smart watches that are web-enabled

Aim

To highlight the responsibility of the school, staff, governors and parents/carers to mitigate risk through reasonable planning and actions. Electronic Safety (e-Safety) covers not only internet technologies, but also electronic communications via mobile phones, games consoles and wireless technology. This policy applies to all members of the school community (including governors, staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of the school.

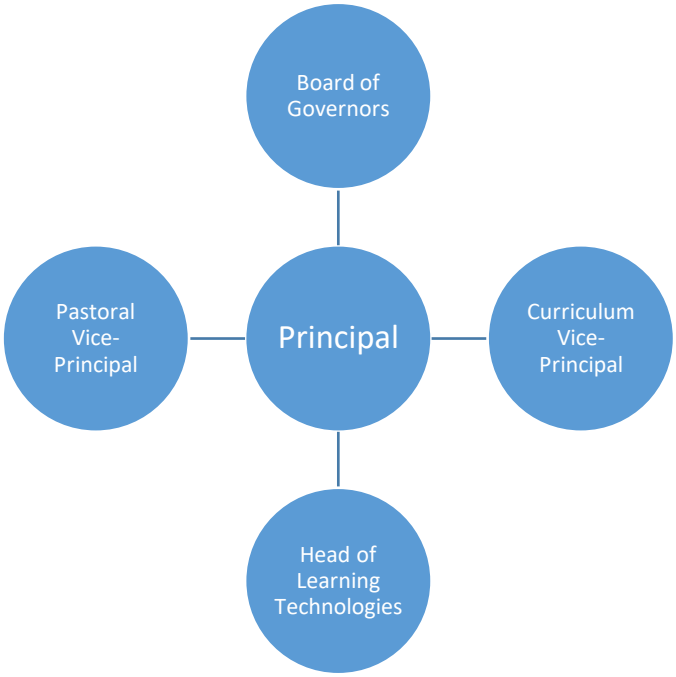
Objectives

E-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world
- emphasises learning to understand and use new technologies in a positive way
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online
- is concerned with supporting pupils to develop safer online behaviours both in and out of school
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately

Roles and Responsibilities

Responsibility Hierarchy



Board of Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about e-safety incidents and monitoring reports. A member of the Governing Board has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include receiving updates from the Head of Learning Technologies on E-Safety incidents and logs.

Principal and Senior Leaders

The Principal has a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for E-safety will be delegated to the Head of Learning Technologies.

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

The Principal/Senior Leaders are responsible for ensuring that the Head of Learning Technologies and other relevant staff will receive suitable training to enable them to carry out their e-safety roles and to train other staff. The Senior Leadership Team (SLT) will receive regular monitoring reports from the Head of Learning Technologies.

The **Head of Learning Technologies** will take day-to-day responsibility for E-safety issues and has a leading role in:

- establishing and reviewing the school E-safety policies and documents
- ensuring that all staff are aware of the procedures to be followed in the event of an e-safety incident taking place
- providing training and advice for staff
- liaising with C2k
- liaising with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to SLT

The **Head of Learning Technologies & IT Technical Staff** are responsible for ensuring that:

- the Belfast Boys' Model School technical infrastructure is secure and is not open to misuse or malicious attack
- Belfast Boys' Model School system meets required E-safety technical requirements
- users may only access the networks and devices through a properly enforced password protection policy, where passwords are regularly changed
- the filtering policy – that it is applied and updated on a regular basis
- they are up-to-date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal/Head of Learning Technologies for investigation.

Teachers, Classroom Assistants and Support Staff are responsible for using Belfast Boys' Model School technology systems in accordance with the Acceptable Use Policy (Staff) and are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the Acceptable Use Policy (staff)
- they report any suspected misuse or problem to the Head of Learning Technologies and Pastoral Vice Principal
- all digital communications with pupils/parents/carers is 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 in their classes
- 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, implementing current policies with regard to these devices

- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Teacher for Child Protection should be trained in E-safety issues and be aware of the potential for serious child protection/safeguarding issues that may 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 Belfast Boys' Model School technology systems in accordance with the Acceptable Use Policy (Pupils). They:

- are responsible for using the school's digital technology systems in accordance with the Acceptable Use Policy (Pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices
- will be expected to know and understand policies on the taking/use of images and their role in cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Belfast Boys' Model School E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet /mobile devices in an appropriate way. Belfast Boys' Model School will take every opportunity to help parents understand these issues through parents' evenings, Parent App, letters, website and information about national/local E-safety campaigns literature. Parents and carers will be encouraged to support the school 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 school

Education

Regulation and technical solutions are very important and their use must be balanced by education. The education of pupils, parents and staff is an essential part of Belfast Boys' Model School's E-safety provision.

Pupils

Pupils need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and 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 classes and will be regularly revisited
- Key E-safety messages will be reinforced as part of a planned programme of assemblies (Safer Internet Day, etc.) and the Pastoral curriculum
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for their Acceptable Use Policy 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 visited

Parents/Carers

Many parents and carers have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Belfast Boys' Model School will therefore seek to provide information and awareness to parents and carers through:

- Letters, website & Parent App
- Parents evenings & awareness events
- High profile events & campaigns e.g., Safer Internet Day

Staff

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

- a planned programme of formal E-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-safety training needs of all staff will be carried out regularly.
- all new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand Belfast Boys' Model School's E-safety policy and Acceptable Use Agreements
- the Head of Learning technologies will provide advice, guidance and training to individuals as required
- staff should understand that phone or digital communications with pupils can occasionally lead to misunderstandings or malicious accusations. Staff must take care always to maintain a professional relationship.

Communication

When using communication technologies Belfast Boys' Model School considers the following as good practice:

- the official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- users must immediately report, to the C2K Manager/Head of Learning Technologies/ICT Technician, the receipt of any communication that makes them feel uncomfortable, or which they feel is offensive, discriminatory, threatening or bullying in nature (and must not respond to any such communication.)
- any digital communication between staff and pupils or parents/carers (email, chat, video conferencing, social media, etc.) must be professional in tone and content
- incoming emails from an unknown source should be treated as suspicious and attachments not opened
- in digital communications students must not reveal their personal details or those of others, or arrange to meet anyone without permission of a parent/ carer.

Social Networking

All schools have a duty of care to provide a safe environment for pupils and teachers. Belfast Boys' Model School provides the following measures to ensure the safety of all:

- pupils are unable to access social networking sites such as Facebook/Twitter/Instagram/TikTok through the C2K network or private WIFI system
- teachers who obtain knowledge of pupils accessing social networking sites via proxy avoidance measures should report this to the Head of Learning Technologies/ICT Technician immediately to have the site blocked
- Belfast Boys' Model School's Facebook, Twitter, Instagram and YouTube accounts have been created to promote the positive life of the school. These are controlled by a member of the Senior Leadership Team.

School staff should ensure that:

- no reference is made in social media to pupils, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not attributed to the school.

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing Internet Access

Internet Filtering

Belfast Boys' Model School is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections are effective in carrying out their e-safety responsibilities:

- Belfast Boys' Model School will work with C2K, Internet Service Provider to ensure that systems to protect students are reviewed and updated regularly.
- all users have clearly defined access rights to Belfast Boys' Model School systems and devices.
- all users are provided with a secure username and password. Users are responsible for the security of their username and password.
- internet access is filtered for all Belfast Boys' Model School users. Content lists are regularly updated and internet use is monitored and logged
- if staff or pupils discover an unsuitable site, it must be reported to the Head of Learning Technologies/IT Technician. Belfast Boys' Model School will take all reasonable precautions to prevent access to inappropriate material and will review its procedures regularly to ensure protection. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a device connected to Belfast Boys' Model School networks. Belfast Boys' Model School cannot accept liability for any material accessed, or any consequences of internet access.

School Website/Published Content

- Staff or pupil personal contact information will not be published. The contact details provided online will be the Belfast Boys' Model School office.
- SLT for Progression will take overall responsibility and ensure that content published is accurate and appropriate.

Digital Images and Videos

Acceptable use of a mobile device in school by pupils

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. For example, such images could potentially result in cyberbullying. Moreover, digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

It is common for employers to carry out internet searches for information about potential and existing employees. Pupils are permitted to bring mobile devices into school on the understanding that they agree with limitations on their use, as stated in the Acceptable Use Policy (Pupils). Belfast Boys' Model School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- parents/carers are welcome to take videos and digital images of their children at Belfast Boys' Model School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/ video images.
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Belfast Boys' Model School policies concerning the sharing, distribution and publication of those images.
- care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or Belfast Boys' Model School into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission.
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- pupil's full names will not be used anywhere on a website, social media or blog, particularly in association with photographs.
- permission from parents/carers will be obtained before photographs of pupils are published on Belfast Boys' Model School website/social media pages.

Cyberbullying

This 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 devices – 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.

It is important that pupils are encouraged to 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 Belfast Boys' Model School Anti-Bullying Policy to monitor the effectiveness of their preventative activities, to review and ensure consistency in their investigations, support and sanctions.

Personal/Cloud Storage

Pupils and staff make use of cloud storage operators such as OneDrive, Google Apps for Education or Dropbox. When using this storage Belfast Boys' Model School considers the following as good practice:

- do not share your username and password
- files brought into Belfast Boys' Model School on pen drives/cloud storage must be relevant and appropriate for educational purposes
- inappropriate content must be reported to the Head of Learning Technologies immediately.

Email Security

- In the school context, email 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.)

Internet Security

- Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. The C2K authentication process 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 school principal.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR

ALC Pupils

For pupils who study in another school within the NBALC, it is the responsibility of the teaching school to provide, within Induction, the school's AUP and relevant procedures within the E-safety policy to ALC pupils The NBALC teaching school will share their E-safety and other relevant policies to the home school through the relevant staff, e.g., Head of Sixth Forms/Vice-Principals.

If an ALC pupil has breached the guidelines of the pupil AUP or the school's E-safety Policy, the teaching school outlines the issue and presents the evidence and the home school follows the procedures and sanctions of their E Safety, AUP and other relevant policies, e.g., positive Behaviour Policy and relevant sanctions. Parents and the teaching school are updated on progress and outcome by home school.

If a Child Protection issue arises out of the breach by the ALC pupil, the Designated Teachers/Vice Principals will communicate and follow the procedures outlined in the teaching school's E-safety policy.

Roving Access

For a staff member or student at a school to get roving access at another school:

- the C2k Manager at the home school must send a roving access request for their staff or students to the destination school
- the C2k Manager at the destination school must then approve the requests from the home school.

Roving Users:

- cannot access the drives from their own school when visiting the destination school
- have a temporary drive for each login session but its contents are erased at the end of each session. It is advisable for roving users to use MyFiles to access their documents while in the destination school.
- will have access to the App Store and default C2k applications
- can access their own MYSCHOOL account through the internet: URL www.c2kschools.net | C2k username and password
- accounts continue to be managed by the home schools. For example, resetting passwords, unlocking accounts, allocating groups, internet access, Meru access etc., are all still managed by your home school even when you are roved
- email will be their home school account.

Dealing with breaches of the guidelines

Misuse of a mobile device will be dealt with using the same principles set out in the Positive Behaviour & Discipline Policy, with the response being proportionate to the severity of the misuse. The Vice Principal/Principal 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 device, 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 device this will be carried out by the Vice Principal/Principal. 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 of a mobile device in school by pupils

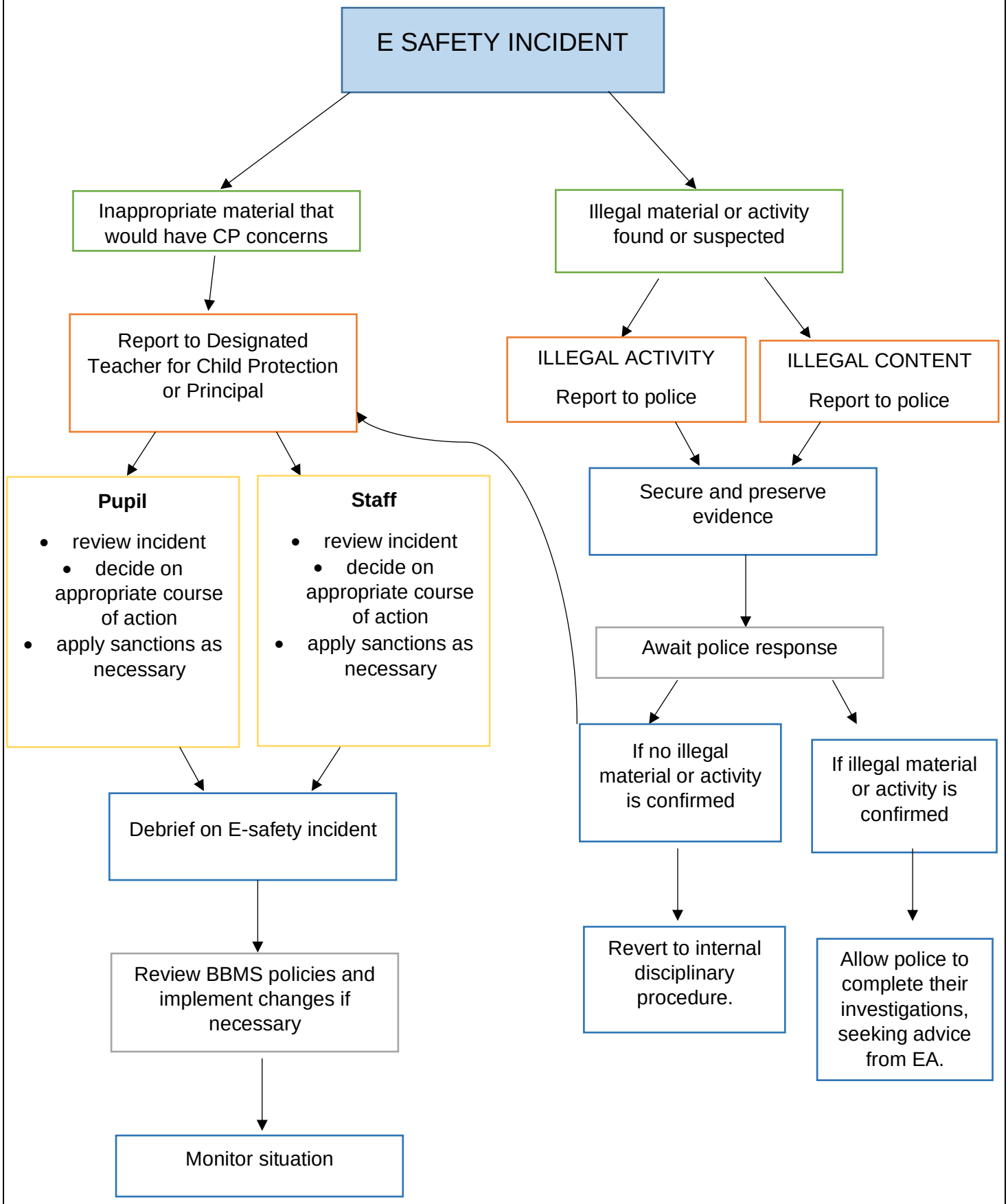
The school will consider any of the following to be unacceptable use of a mobile device:

- Photographing or filming staff or other pupils without their knowledge or permission
- Photographing or filming in toilets, 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 mobile device off or handing over the mobile device at the request of a member of staff.

Using a mobile phone device outside of school hours to intimidate staff or pupils will also be considered a breach of these guidelines.

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 Education Authority Child Protection Team and/or the PSNI. The Principal will consider whether an incident should be reported to the Designated Teacher for Child Protection.

The Designated Teacher for Child Protection will 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. The flowchart for dealing with an E-safety incident is detailed on the following page.


E SAFETY INCIDENT
Inappropriate material that would have CP concerns
Illegal material or activity found or suspected
Report to Designated Teacher for Child Protection or Principal
ILLEGAL ACTIVITY
Report to police
ILLEGAL CONTENT
Report to police
Pupil
review incident
decide on appropriate course of action
apply sanctions as necessary
Staff
review incident
decide on appropriate course of action
apply sanctions as necessary
Secure and preserve evidence
Await police response
If no illegal material or activity is confirmed
If illegal material or activity is confirmed
Debrief on E-safety incident
Review BBMS policies and implement changes if necessary
Monitor situation
Revert to internal disciplinary procedure.
Allow police to complete their investigations, seeking advice from EA.

Procedures for E-Safety Policy Review

The procedures for E-Safety Policy review are:

1. Make sure you need the policy – did the policy achieve its objectives and are these still relevant
2. Check for key changes in guidance
3. Understand whether the policy is working effectively
4. Consultation with those affected by policy, e.g. pupils, parents/carers, staff
5. Consult on any major changes

Consultation for Policy Development

The consultation for Policy Development will include:

- Consultation with stakeholders – parents/carers, staff
- Input from pupils via Student Council

Appendix I

Relevant DENI documents

DE Circular 2007/01: Acceptable Use of the Internet and Digital Technologies in Schools

DE Circular 2011/22: Internet Safety (Addendum to 2007/01)

DE Circular 2013/25: eSafety Guidance

DE Circular 2016/26: Effective Educational Uses of Mobile Digital Devices

DE Circular 2016/27: Online Safety

Appendix II

Legal Framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Public Order (NI) Order 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) (NI) 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 victims actual or presumed religion, race, sexual orientation or disability.

Protection of Children (NI) 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 (NI) 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 (NI) 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).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

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 programs 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.

Cyber-bullying

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

Appendix III

Relevant Guidance Documents

Northern Ireland Executive: Online Safety Strategy: Keeping children and young people safe: an online safety strategy for Northern Ireland 2020-2025.

CPSS E-safety Policy guidance

Appendix III

Relevant linked school policies

Staff and Pupil Acceptable Use Policies

Blended and Remote learning Policy

Data Protection Policy

Pastoral Care Policy

Safeguarding and Child Protection Policy

Positive Behaviour Policy

Anti-Bullying Policy

Appendix IV

Risk Assessment

Proposed responses to e-safety incidents by children

No.	Activity	Hazard	Likelihood	Impact	Score	Further controls
1.	Internet browsing on a managed device	Access to inappropriate / illegal content - **staff**	1	3	3	
2.	Internet browsing on a managed device	Access to inappropriate / illegal content - **pupils**	2	3	6	
3.	Blogging on a managed device	Inappropriate comments	2	2	4	
4.	Blogging on a managed device	Using copyright material	2	2	4	
5.	Pupil laptops	Pupils taking laptops home – access to inappropriate/illegal content at home	2	3	6	Risk management needed by ICT department
6.	BYOD	Inappropriate/illegal content brought into school	3	3	9	Risk management needed by ICT department

Risk Assessment

Likelihood: How likely is it that the risk could happen

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: **1 – 3 = Low Risk**

4 – 6 = Medium Risk

7 – 9 = High Risk