HUNTERHOUSE COLLEGE

E-SAFETY POLICY

Date/date Reviewed: **2020**

Date Ratified: **October 2020**

Previous: **2017**

Next Review Due: **2022**

This policy is available in pdf format from the College website

www.hunterhousecollege.org.uk

or on request from the College Office 028 9061 2293

info@hunterhousecollege.belfast.ni.sch.uk

Inclusion & Diversity:
The College aims to establish an inclusive community where all students and staff are treated with dignity and respect, regardless of individual differences including, but not limited to, culture, race, religion, beliefs, sexual or gender orientation, appearance, ability or disability.

Rationale:
The College recognises and values the increasingly wide range of opportunities that information technology provides to our staff and students. Whilst it is our aim that all members of our school community avail as fully as possible of this technology, we also appreciate the need for safeguards to be in place. Mobile devices and, in particular, the new generation of smart phones, such as the iPhone, now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet.

Information and Communications Technology (ICT) in school includes a wide range of resources such as web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail and Instant Messaging
- Chat Rooms and Social Networking such as Facebook, Snapchat and Twitter
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices such as IPads with web functionality

Young people have many opportunities to benefit from what are becoming very sophisticated hand-held devices outside school. The College recognises that this will provide useful skills and opportunities in the future.

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Hunterhouse College want to create a safe ICT learning environment. C2K, who manage our computer systems, have a wide range of resources available to help address potential internet safety problems. However, technological tools are effective only when used in the context of a comprehensive internet safety programme, as outlined below.

While a number of the issues outlined in this policy relate, primarily, to ICT use outside school, it is inevitable that some of the issues, when initiated outside school, will be bought back in and need to be dealt with accordingly by the College. For example, bullying via chat or text messages will impact upon relationships within school; obsessive use of the internet may impact upon the quality of schoolwork. Changes in the personality and general well-being of a student may indicate that they are involved in inappropriate or illegal behaviours online.

One of the key safeguards the College uses is Securus software which is provided by C2K. This monitors, at a key stroke level, all usage of c2k machines by students while on the College site. Daily reports of any concerns are sent to key staff who are then able to act upon any concerns appropriately.

Aims:
The creation of a safe learning environment for all members of the school community through:

- an infrastructure of whole-school awareness, designated responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive internet safety education programme for the whole school community

Roles & Responsibilities:

Board of Governors:
The Board of Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out every two years by the Governors who receive regular information about e-safety incidents and monitoring reports via the Safeguarding Termly Reports to Governors. A member of the Governing Board has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety teacher
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Board of Governors meeting

Principal and Senior Leaders:
The Principal (Mr A. Gibson) 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 Designated Teacher in charge of E-Safety (Mr N. Goodall).

The Principal and (at least) another member of the Senior Leadership Team 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.

The Principal is responsible for ensuring that the E-Safety teacher and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Senior Leadership Team will receive regular monitoring reports from the E-Safety teacher.

Staff:
Teaching 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 report any suspected misuse or problem to the Principal, a Designated Teacher/Deputy Designated Teacher or E-Safety Teacher for investigation/action/sanction

- they are aware that all digital communications with students and parents/carers should be on a professional level and only carried out using official College systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety, Mobile Phone and Acceptable Use Policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they act as good role models in their use of digital technologies, the internet and mobile devices
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other College activities (where allowed) and implement 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.

E-safety Teacher:

Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents as follows:

- 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 the C2K
- liaises with school technical staff
- receives reports of e-safety incidents from Securus and creates a log of incidents to inform future e-safety developments
- attends any relevant Governor meetings.
- reports regularly to Senior Leadership Team.

ICT Technicians:

The ICT Technical Staff are responsible for ensuring:

- that the college's technical infrastructure is secure and is not open to misuse or malicious attack
- that the college meets required e-safety technical requirements and any Education Authority E-Safety Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep 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 required
- that the use of the network/internet/Virtual Learning Environment/remote access/email provided to the school by C2K, is regularly monitored in order that any misuse/attempted misuse can be reported to the appropriate person for investigation.

Designated/Deputy Designated Teachers:

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

Students:
All students will be regularly made aware of the importance of adopting good e-safety practice when using digital technologies both inside and 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 College.

At Hunterhouse College, it is expected that students:

- are responsible for using the college digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of and steps to follow for reporting;
    - abuse
    - misuse
    - access to inappropriate materials
- will know and understand policies on the use of mobile devices and digital cameras including the likely sanctions for breaking them. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- 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 College.

Parents/Carers :
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The College will take every opportunity to help parents/carers understand these issues through information evenings, letters, the school website and information about e-safety campaigns/literature. Parents/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
- their children's personal devices in the school.

The following websites should be helpful and give more information:

http://www.beatbullying.org/
https://www.net-aware.org.uk/
https://www.thinkuknow.co.uk/assetslibrary/
http://www.childline.org.uk/explore/onlinesafety/Pages/OnlineSafety.aspx
http://www.thinkuknow.co.uk/

E-safety Procedures:

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

E-safety is therefore a focus in all areas of the curriculum and staff in all subjects reinforce e-safety messages across the curriculum as follows:

- Key e-safety messages are reinforced as part of a planned programme of assemblies and through the Personal Development curriculum
- Students are taught in all subjects to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked or triggering Securus. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study.

Parents/Carers:
Many parents and carers may 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, including on social media sites, and may be unsure about how to respond.

The College therefore seeks to provide information and awareness to parents and carers through:

- Curriculum activities
- Parentmail, Twitter and the College website
- Parents/Carers information evenings
- High profile events and campaigns e.g. Safer Internet Day

Infrastructure, Filtering and Monitoring of ICT Usage:
The College is responsible for ensuring that the College's infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This also includes ensuring that the relevant people named in the above sections are effective in carrying out their e-safety responsibilities.

Hardware and Software:

- Hunterhouse College's technical systems are managed in ways that ensure that the College meets recommended technical requirements
- There are regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling is securely located and physical access restricted
- All users have clearly defined access rights to the College's technical systems and devices
- All users are provided with a username and secure password by the ICT Technicians who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password when specified by C2K
- The 'Administrator' passwords for the College's ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. school safe)
- College technical staff will be responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

Filtering and Monitoring:
The College utilises the resources (both Hardware and Software) provided by C2K. The systems implemented by this group include filtering and monitoring which are outlined in the C2K Information Sheet EN074 (Acceptable Use Policy for C2K Services).

- Throughout the C2K System, Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images). Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The College has provided differentiated user-level filtering, allowing different filtering levels for different stages and different groups of users – staff/ students etc.
- College technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and workstations are protected by up to date virus software.
- An agreed security system is in place that allows/forbids users from downloading executable files and installing programmes on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Any attempts to bypass filtering, or to access inappropriate or illegal material, will be reported to the school authority via C2k.
- Email messages are subject to C2k's filtering policy.

Bring Your Own Device (BYOD):
The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, a number of e-safety considerations for BYOD have been reviewed prior to implementing such a strategy. The College strives to ensure that the use of BYOD should not introduce vulnerabilities into existing secure environments.

- The College has a set of clear expectations and responsibilities for all users
- The College adheres to the General Data Protection Regulation principles
- All users are provided with and accept the Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the college's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy

Use of digital and video images:
The development of digital imaging technologies has created significant benefits to learning. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place.

The College 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 students 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the General Data Protection Regulation (GDPR)). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking video/images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute. Guidance will be issued to students as to how they will appropriately engage in video chats with staff as part of remote learning.
- Students must not take, use, share, publish or distribute images of others without their permission. This includes capturing images from video-based lessons on Microsoft Teams or other methods of video chat which have been approved by the Principal.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with parental consent for the use of such images.
- Written permission from parents or carers will be obtained on admission to the College for photographs of students that are published on the school website or other social media site

Links to Other Policies:
Acceptable Use Policy
Anti-Bullying Policy
Mobile Phone Policy
Positive Behaviour Policy
Safeguarding & Child Protection Policy – including COVID-19 Addendum
Student Progress Policy
Suspension & Expulsion Policy

Appendix 1

The Legal Framework

This section shows the context upon which the above e-Safety Policy is based. It 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 (N.I.) 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) (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.

Sexual Offences (N.I.) order 2008

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)
Persons 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.

Data Protection Act 1998 (Replaced by General Data Protection Regulation May 25th 2018)

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).

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.

Regulation of Investigatory Powers Act 2000

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, 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

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

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

Appendix 2

Mobile Phone Policy

HUNTERHOUSE COLLEGE MOBILE PHONE POLICY (updated June 2020)

This policy has been drawn up with the interests of the whole college community in mind and with the intention of safeguarding students and preventing disruption to learning.

Any infringement of this policy will result in sanctions being applied which may involve confiscation of the phone

Students will be reminded regularly of steps to take to safeguard themselves while using mobile phones and other personal electronic devices. While it is not the remit of the College to investigate inappropriate use of mobile phones/social media outside the College, we would ask parents/carers to make us aware of any such incident and will we work to support any student in College affected by this. We will also liaise with outside agencies investigating any such incident. Students should be aware that inappropriate use of social media sites either inside or outside of College may involve the PSNI, Social Services and other agencies.

1. If any parent/carer wishes their child to have a mobile phone when they are on the College site, then s/he should complete the Mobile Phone reply slip. This requires the student and parents/carers to acknowledge by signing that they understand and accept the College's Mobile Phone Policy.
2. The College cannot accept responsibility for loss or damage to property, however that loss or damage may be deemed to have been caused.
3. **When a student is on the College site, their phone should be switched onto silent mode and out of sight in their inside blazer pocket.** If a member of staff sees a student with a visible mobile phone around the College site, they will be asked to put it in their inside blazer pocket.
   Repeated instances will lead to the confiscation of the phone. If a student gets their mobile phone out in a lesson, unless they have been directed to do so for an educational purpose by a member of staff, the phone will be confiscated by the member of staff and held in Pupil Reception.
   The student may collect the phone at the end of the day and they will receive a Concern Point. Please note that Sixth Form students may use their phones in the Sixth Form Leisure Area only.
4. At no point should a student use their mobile phone (or other personal electronic device) to take photographs/videos of other members of the College community unless they have been authorised to do so. **Students should be aware that it is an offence to film/photograph another person without their permission**. Any student who uses their mobile phone in school to film/photograph another person without their permission will be subject to serious sanctions and may be referred to the PSNI.

5. If a student feels that they need to contact a parent/carer at any point during the school day they should come to Pupil Reception where arrangements will be made to enable them to do this.
6. If contact with parents/carers needs to be made because a student is unwell or has had an accident, this will be done by College staff via Pupil Reception/Main Office. It is not acceptable for a student to use their mobile phone to contact parents/carers directly to ask to be taken home without the knowledge of a member of staff.
7. Parents/carers needing to contact a student during the school day should contact Pupil Reception/Main Office.

✂ ----------

Reply Slip **Use of Mobile Phones**

Name of Student: …….

Their mobile phone number is: ……..

Please tick below as appropriate.

My child's phone has internet access. I have reminded them that they must not use their phone to access social networking sites while they are on the College site.	
If my child needs to access the internet during the school day, they are aware that filtered internet and monitored internet access is available via the computers in the LRC, including at break, lunchtime and after school.	

- I/We have read and understood the College's Mobile Phone Policy.
- I/We understand that the Mobile Phone Policy was drawn up with the interests of the whole college community in mind and with the intention of safeguarding students and preventing disruption to lessons and to school routines.
- I/We understand that any infringement of this policy will result in sanctions being applied which may involve the phone being confiscated.
- I/We understand that if a student is found in possession of a mobile phone (or other personal electronic device) during an examination, either internal or external, they are likely to have their paper cancelled. A public examining body may, in such circumstance, ban a candidate from taking any of that authority's examinations in future or may cancel any marks which have been awarded in previous papers in that examination series.
- I/We undertake to notify the College if the students' mobile phone number changes.

Signed:
(Parent/Carer) _____ Date: _____

Signed:
(Pupil) _____ Date: _____

Appendix 3

Temporary Use of C2k Wifi Agreement on Non-School Devices

You have requested access to the C2k Wifi facility available within the school under the Bring Your Own Device (BYOD) scheme.

This access can be granted on the following being agreed to:

1. The access is granted only until the end of the current academic year ie until 30 June 2021
2. Students using this facility must agree to the school's Acceptable Use of Internet Policy (AUIP)
3. Access is granted for educational purposes only and students should not attempt to access other types of site including those which would be described as 'Social Media' unless such access has been requested by a member of staff for educational purposes.
4. Access will be subject to C2k filtering but if a student becomes aware of a site containing unacceptable material being available, the College will be informed so that steps can be taken to block the site.
5. Access is granted to individual students only. Once granted, students must not allow their account to be used by others to access the C2k Wifi.
6. The College cannot accept any responsibility for loss or damage to devices brought onto College premises under the BYOD scheme. Students should therefore ensure that they take adequate steps to protect their devices from loss or damage and, if necessary, have insurance to cover loss or damage to devices.

I have read the conditions above and am requesting access to the C2k Wifi under the BYOD scheme.

Signed _____

Name _____

Form _____

Date _____

Permission granted Y/N

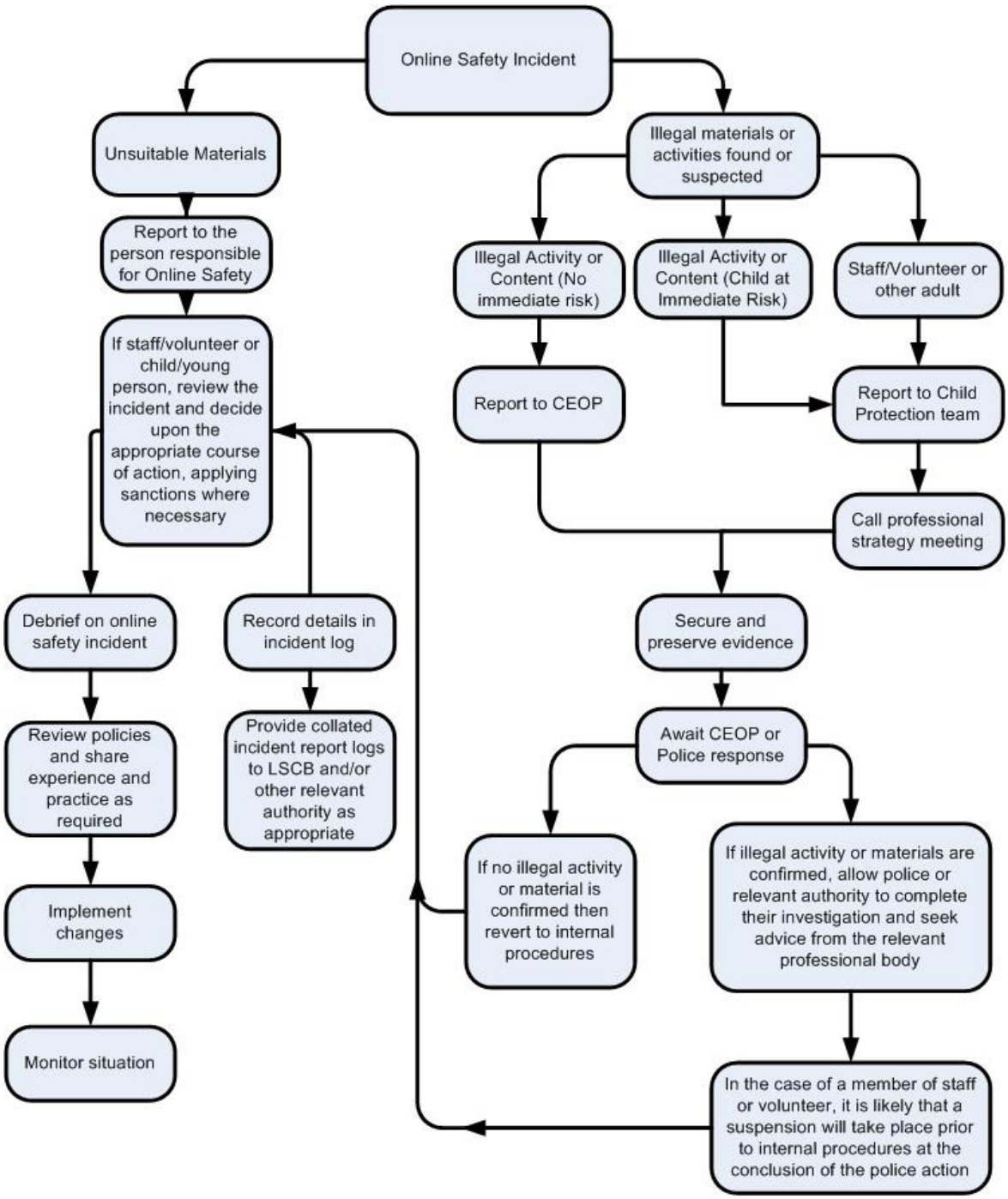
Signed _____

Date _____

Appendix 4

Guidelines for Responding to Illegal Incidents

If there is any suspicion that a website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to the PSNI.



Appendix 5

Examples of Breaches of the Policies:

- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone/digital camera/other personal electronic devices
- Unauthorised use of social media/messaging apps/personal email
- Unauthorised downloading or uploading of files
- Taking an image/video of another member of the College community without their permission
- Sharing an image/video of another member of the College community without their permission
- Posting an image/video online of another member of the College community without their permission
- Existence of images/videos of students in College uniform and/or taken on the College site without staff permission, including the sharing of or posting online of any such images/videos
- Unauthorised downloading or uploading of files
- Allowing others to access the College network by sharing username and passwords
- Attempting to access or accessing the College network using another student's account
- Attempting to access or accessing the College network using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the College into disrepute or breach the integrity of the ethos of the College
- Using proxy sites or other means to subvert the College's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR

Appendix 6

Risk Assessment for Devices outside of C2K

Rational to Risk Assessment:

As mobile technology becomes a dominant force in the education sector, Hunterhouse College have established a Bring Your Own Device (BYOD) scheme that permits students to bring their own laptop or tablet device to school to be used as a digital learning device.

There are many logistical, financial and educational advantages to implementing a BYOD scheme at your school. However, there are many pitfalls to consider. Therefore, the College introduced an effective BYOD policy that represents the best interests of both the school and the students and has completed the following Risk Assessment**.**

With the fast pace of technological development Hunterhouse will continue to develop and enhance this and relating BYOD working documents, striving to reduce the risk to Students and Staff as much as possible.

Potential Risk	Environment in which the risk occurs	Element of Risk	Preventative Strategies	Reactive Strategies
Capturing and Distributing Original Digital Images (Video, photographs, sound recordings etc).				
Capturing images and /or videos of student	Classrooms, Corridors, Toilets, Changing rooms Lunch time facilities	Likely, large number of student presents high student to staff supervision ratio.	Students will be made fully aware of the College's Mobile Phone Policy which is included in their school planners. Students will be made aware of E-Safety Policy which contains the clear guidelines for the use of personal devices to capture images. Use of Assemblies and PD sessions to highlight the laws relating to capturing images.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents Notified. • PSNI notified (If applicable). • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.
Capturing images and/or videos of staff	Classrooms, Corridors	Unlikely, level of supervision high	Students will be made fully aware of the College's Mobile Phone Policy which is included in their school planners. Students will be made aware of E-	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • PSNI notified (If applicable).

			Safety Policy which contains the clear guidelines for the use of personal devices to capture images. Use of Assemblies and PD sessions to highlight the laws relating to capturing images.	• Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.
Distributing Images by Posting on Social Media (WhatsApp, Snapchat, Facebook, Twitter, etc).	Form Rooms Lunchrooms/ areas Recreation area Corridors Toilets	Highly likely, very limited opportunities for staff monitoring	Students will be made fully aware of the College's Mobile Phone Policy which is included in their school planners. Students will be made aware of E-Safety Policy which contains the clear guidelines for the use of personal devices to capture images. Use of Assemblies and PD sessions to highlight the laws relating to the distribution of images.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • PSNI notified (If applicable). • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.
Distributing Images by showing others.	Form Rooms Lunchrooms/ areas Recreation area Corridors Toilets	Highly likely, very limited opportunities for staff monitoring	Students will be made fully aware of the College's Mobile Phone Policy which is included in their school planners. Students will be made aware of E-Safety Policy which contains the clear guidelines for the use of personal devices to capture images.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • PSNI notified (If applicable). • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.

			Use of Assemblies and PD sessions to highlight the laws relating to the distribution of images.	
Distributing Images of students for other schools	Form Rooms Lunchrooms/ areas Recreation area Corridors Toilets	Unlikely, very limited opportunities for staff monitoring.	Students will be made fully aware of the College's Mobile Phone Policy which is included in their school planners. Students will be made aware of E-Safety Policy which contains the clear guidelines for the use of personal devices to capture images. Use of Assemblies and PD sessions to highlight the laws relating to the distribution of images.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • Other School contacted (if applicable due to safeguarding). • PSNI notified (If applicable). • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.
Internet Access Using Mobile Data (Outside of C2K filtered network)				
Accessing Internet using Mobile Data	Lunchrooms/ areas Recreation area Corridors Toilets LRC	Highly likely, large number of student presents high student to staff supervision ratio.	Students will be made fully aware of the College's Mobile Phone Policy which is included in their school planners. Students will be made aware of E-Safety Policy which contains the clear guidelines for the use of personal devices to access the internet using Mobile Data.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.
General Risks of Bringing Your Own Device scheme				
Accessing sites containing unacceptable	Within the C2K Wi-Fi Network	Unlikely, devices connected to the network are	Students will be made aware of E-Safety Policy and	• Phone/Device Confiscated. • Removal of BYOD

material using C2K network		subject to the C2K filters.	AUP which contains the clear guidelines for the use of personal devices to capture images.	privilege. • Parents/Carers Notified. • Further reminder of the College rules in both form time and assemblies.
Loss or damage of device	Whole School Campus	Likely due to the movement between lessons.	Students made aware of the risk to their property when they complete the BYOD agreement document.	• Referral to the BYOD agreement which was signed. • Further reminders to all students about the need to be careful of their devices when bringing them into the College.
Device containing inappropriate images/content	Whole School Campus	Likely, large number of students presents high student to staff supervision ratio.	Students are made aware of the filtering systems which are run in school by C2K. Students are made aware of the laws and rules governing images on their devices.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • PSNI notified (If applicable). • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.
Device containing Viruses/Malware	Within the C2K Wi-Fi Network	Unlikely, devices connected to the network are subject to the C2K filters.	Students are made aware of the filtering systems which are run in school by C2K. Students are educated on how to protect themselves and their devices from Malicious Software. Students are made aware of the laws and rules governing virus on their devices.	• Phone/Device Confiscated. • Removal of BYOD privilege. • Parents/Carers Notified. • PSNI notified (If applicable). • Phone/Device to be checked in to Pupil Reception during school hours. • Further reminder of the College rules in both form time and assemblies.