E-SAFETY and ICT ACCEPTABLE USE POLICY

Belfast High School

Date: **May 2025**

Date Ratified: **28 May 2025**

Ratified by: **Board of Governors**

Responsibility: **Board of Governors**

Author: **Vice Principal**

Review Date: **May 2028**

Introduction

This policy acknowledges and complies with DE Circulars 1999/25, 2007/01, 2011/22, 2013/25, 2016/26 and 2016/27.

Rationale

Belfast High School recognises that ICT and the internet are effective tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, support creativity and develop independence. Using ICT can be beneficial, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents/carers use it appropriately and practise good e-safety. It is important that all members of the School community are aware of the dangers of using the internet and know how they should conduct themselves online.

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a significant part of everyday life, education and business. The School wants to equip pupils with all the necessary ICT skills that they will need to enable them to progress confidently into a professional working environment when they leave school.

ICT Facilities in Belfast High School

Belfast High School has many computers, printers and scanners throughout the School. Pupils are encouraged to make use of the managed network for all aspects of their work. Filtered internet access is available at every station and all pupils have a secure C2K email account. This is the only email account that pupils may use in school and for school related matters.

Before a pupil can use the network, send a school email or access any internet site it is important that they and their parents/carers have read and fully understand these terms and conditions of use and the relevant parental consent has been provided.

The network is a learning and teaching tool to support school studies. It is not a recreational medium and should not be used as such.

Usernames and Passwords

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

To access the School network, each pupil has a unique username and password. Pupils should remember their username and password and keep these secure at all times. It is not a good idea to write passwords down. All pupils will be held accountable for the data that is stored in their network area and for activities that are carried out in their name.

The School ICT Manager may be contacted in the Harte Building if pupils have enquiries about passwords. Pupils should bear in mind that systems policies dictate that passwords are changed every 90 days; however, if a pupil feels that his/her password has been compromised it can be changed by holding down Ctrl and Alt and pressing Delete.

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

- By saving work on to a USB memory stick or portable hard drive. Pupils should write their names on memory sticks if possible, otherwise re-name the device using their own name. For documents containing personal data, staff must either password protect the USB memory stick using 'Bitlocker' (or similar software), or password protect any documents or files containing personal data;
- By email attachment although this will be subject to filtering;
- By logging on directly to their 'C2K Documents' from home;
- By usingGoogle Classroom, Microsoft Teams, One Drive or other web based workspace;
- By using the cloud-based storage options available to pupils through the C2K network

It is good practice to save work in at least 2 places for backup purposes.

Print credits
Pupils receive a number of print credits each year. These can be supplemented by the purchase of additional printer credits from the School ICT Manager. Pupils may check their personal print credits on the computer desktop.

Listening to Sound
Headphones should be used to listen to sound on any of the School network computers under teacher supervision. In-ear headphones should not be shared.

Email
C2k issues every member of staff and pupil with an email address.
There are 2 versions of the email address, *aperson*123@belfasthigh.newtownabbey.ni.sch.uk and *aperson*123@c2kni.net, both of which can be used.

Staff should be aware of the following regarding the use of school email:

- Use official school-provided email accounts only to communicate with pupils, parents/carers and to conduct other School business. Personal email accounts should not be used to contact any of these people;
- Send professionally and carefully written emails from school accounts;
- Inform the relevant line manager or a member of the Senior Leadership Team if offensive, threatening or unsuitable emails are received, either from within the School or from an external account. Staff should not attempt to deal with this themselves.

Pupils should be aware of the following regarding the use of school email:

- Use school-approved email accounts only (with the exception of UCAS applications);
- Social emailing will be restricted;
- Inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. Pupils should not attempt to deal with this themselves;
- Be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated on the use of email and the associated risks through the ICT curriculum and the preventative curriculum.

E-Safety and The Curriculum

The importance of e-safety is emphasised across the curriculum and pupils are educated n the benefits and dangers of the internet and how to use it in a safe and productive way. Pupils are all made fully aware of the School's code of conduct regarding the use of ICT and technologies and behaviour online.

In lessons where internet usage is planned, pupils will be guided to suitable sites; where pupils are permitted to freely search the internet, staff will be vigilant and monitor the content of websites pupils search.

E-safety and appropriate internet usage messages are delivered through Year 8 Digital Literacy classes, through the Personal Development programme, through assemblies and by external speakers.

Where a pupil/pupils fail to demonstrate appropriate levels of e-safety, the matter will be dealt with in line with the School's Promoting Positive Behaviour for Learning Policy or other policies/procedures as appropriate.

Social Media

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

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. Online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that pupils are educated so that they can make their own informed decisions and take responsibility for their conduct online.

Pupils should take great care with the opinions which they express and content which they include on social media. The School takes no responsibility for items that are uploaded to such sites by pupils out of school hours and out of school. However, the School will take appropriate action against any member of the School community who brings the School into disrepute on a website which can be viewed publicly.

All members of the School community, including parents/carers, are asked to be sensitive to the privacy of others and to report any abuse or any potential case of cyber-bullying. Cyberbullying, as with any other form of bullying, is taken very seriously by the School. Information about specific strategies in place to prevent and tackle bullying are set out in the *Anti-Bullying Policy*. The anonymity that can come with using the internet can sometimes make people feel safe to say and do things that they otherwise would not do in person. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in relevant action being taken. The *Anti-Bullying Policy* is available on the School website: www.belfasthigh.org.uk.

All reputable websites have a section for reporting abuse. The School website contains a link on the home page to the CEOP Internet Safety website with information on staying safe online. E-Safety guidance for pupils can also be found in Appendix 1.

Risks Associated with Internet Access

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

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

C2K and the School work together to provide filtered access to the internet. This means that searches for certain keywords will be denied as will access to particular sites. This filtering extends to the system 'reading' the content of pages accessed, and determining whether the information contained is appropriate for use in school. The filtering system in use records each and every website visited along with anything that has been requested.

Virtual Learning

All Belfast High School, pupils have access online workspaces such as Google Classroom, Microsoft Teams and One Drive. All information, including pictures, stored on these workspaces are secured by password and are copyright protected**.** The use of these workspaces greatly enhances the opportunities for 'anytime', 'anywhere' learning in a structured and independent way. They can contain course information, online content, communication tools, online submission of work and subsequent feedback, tracking facilities, links and much more.

Managing Emerging Technologies and Artificial Intelligence (AI)

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

We recognise the role that AI can play in schools as a supportive tool to enhance learning, creativity, and research while ensuring its responsible and ethical use. Pupils and staff must critically evaluate AI-generated content for accuracy, bias, and reliability, avoiding over-reliance on AI for research or decision-making.

With an increased use of AI in daily life, pupils are encouraged to become aware of its potential benefits. The School will support pupils in learning about the appropriate use of AI and the consequences of failing to use AI appropriately e.g. for plagiarism of Controlled Assessment which is dealt with through the Managing Malpractice Policy; the potential for AI bias in shaping pupils' learning and understanding; and the implications of privacy and the need to protect personal and sensitive information when using AI. Staff should guide pupils on safe AI practices, promoting digital literacy and responsible use to maximise benefits while minimising risks.

Using the Network

Pupils are responsible for good behaviour whilst using the network and general school rules apply. This must be borne in mind, especially when pupils communicate with one another online.

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

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

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

Terms of Use
The following are not permitted:

- Eating or drinking at a computer;
- Using any software not registered with the School, including downloads;
- Changing settings on any computer;
- Adding or removing items of hardware without permission;
- Sending or displaying offensive messages or pictures;
- Using offensive or obscene language;
- Activity which threatens the integrity of the School computer system, or activity which attacks or corrupts other systems;
- Activities which are not relevant to the School curriculum;
- Violating copyright laws including downloading, saving or sharing music/video files;
- Accessing the network using any password except your own;
- Disclosing your password to anyone else;
- Trespassing in others' folders, work or files;
- Use of the network or any School computer to access and/or download inappropriate material on the internet;
- Any other misuse as determined by the School.

All emails filtered by C2K software may be read by the system's administrators before they are released.

Violations of any of the rules above may result in temporary or permanent exclusion from the network or the withdrawal of equipment on loan. Parents/carers will usually be informed in writing if an exclusion from the network takes place and may be asked to request reinstatement. Parents/carers may also be invited into school to discuss the problem and in extreme cases will be supplied with copies of the offensive materials.

Use of Personal Equipment
Some pupils may find it helpful to bring in internet enabled devices for use in class when permitted.

The School will, as far as possible, endeavour to provide facilities for these pupils but ultimately the School cannot be held responsible for any losses or breakages; pupils who bring in any personal device do so at their own risk. Any pupil planning on bringing internet enabled devices to school should ensure that they have read and understood the *Bring Your Own Device Policy* and have signed the *Consent Form* before doing so.

The current school policy states that phones must not be seen nor heard during the school day. The only exception is when pupils access the School's wireless network using their own device when directed to by a teacher. Pupils who use their phone outside of this permitted activity during school will receive a sanction in line with the *Promoting Positive Behaviour for Learning Policy.*

Access to Computers in School

- Pupils will have access to computers during ICT classes; staff may book computer suites to facilitate the use of ICT in other lessons.
- Computers in other areas may only be used out of class time if a teacher is present.
- At no time may any food/drink be taken into computer rooms.
- Pupils should not be present in computer rooms without adequate supervision.

Protecting Personal Data

The School takes the protection of personal data very seriously and believes that protecting the privacy of staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The School collects personal data from pupils, parents/carers, and staff and processes it in order to support teaching and learning, monitor and report on pupil progress, and strengthen pastoral provision. The School takes responsibility for ensuring that any data that is collected and processed is used correctly and only as is necessary. Policies and procedures are compliant with the General Data Protection Regulations 2018; further information is available in the School's *Data Protection Policy* and in the Privacy Notices; both are available on the School website.

Using Pupil Images and Work

Images of pupils and pupil work will not be displayed in public, either in print or online, without consent. On admission to the School parents/carers will be asked to sign a consent form. Parents/carers may withdraw consent at any time. Staff may capture and/or use moving/still images of pupils, for whom parental permission has been appropriately received, for display purposes and publicity in and outside school, in School publications, on the School screens and website. Images may be distributed to external media providers for School publicity purposes. Additional consent forms will be required for any external organisation requesting images of pupils.

Staff should ensure that any images of pupils stored digitally should be stored on the C2k network. Staff must transfer digital media from capture devices to the C2k network at the earliest possible opportunity; it is expected that digital images of pupils should be deleted from portable devices as soon as possible. It should not be normal practice to store images of pupils on digital media devices, in a printed format or on any external memory device, for any longer than is necessary.

E-Safety Responsibilities

Staff should:

- read and promote the School's *E-Safety and ICT Acceptable Use Policy*;
- be familiar with the suite of pastoral policies including Safeguarding and Child Protection, Positive Behaviour, Anti Bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately;

- ensure they know what to advise a child who reports a concern relating to any communication or material he/she has received online;
- be responsible for ensuring the safety of personal and confidential school data and information: USB sticks should be encrypted/files containing sensitive or personal data should be password protected;
- observe pupils carefully when using technology or conducting online searches;
- remind pupils that their use of the internet is monitored and that they should not share usernames and passwords;
- maintain a professional level of conduct in their use of technology;
- report all e-safety incidents to a member of the Designated Team.

Pupils should:

- read and adhere to the *E-Safety and ICT Acceptable Use Policy* and follow all safe practice guidance;
- develop an understanding of the risks posed by the use of technology and take responsibility for their own use of technology both inside and outside school (Appendix 1);
- be responsible for ensuring the safety of personal information: USB sticks should be encrypted / files containing sensitive or personal data should be password protected;
- avoid sharing their password with any other person;
- show respect to others in their use of technology both in school and at home;
- develop and understanding of what they should do if they feel uncomfortable or at risk when using technology;
- discuss e-safety with family and friends;
- report any e-safety concerns to a member of staff.

Parents/Carers should:

- read the *E-Safety and ICT Acceptable Use Policy* with their children;
- help and support the School in promoting E-Safety;
- develop an understanding of e-Safety risks and an awareness of the guidance available to support pupils and parents/carers (Appendix 1);
- contact the School if they have any concerns regarding their child's safety.

E-Safety Advice for Pupils

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

Netiquette: a handy guide for teachers and pupils when learning online

The word netiquette is a combination of 'net' (from internet) and 'etiquette'. It means respecting other users' views and displaying common courtesy when posting your views to online discussion groups. Please familiarize yourself with the following points:

Behind Every Name There is a Person:

- Respect the views of class members and what they share in class.
- Ask for clarification if you find a discussion posting difficult to understand. If you come across a posting you regard as offensive, report this to your teacher.
- Avoid sweeping generalizations. Back up your stated opinions with facts and reliable sources.
- Understand that we may disagree and that exposure to other people's opinions is part of the learning experience.
- Be respectful of each other. Before posting a comment, ask whether you would be willing to make the same comment to a person's face.
- Keep in mind that everything you write, indeed every click of your mouse is recorded on the network server. On the Internet there are no take backs.
- Keep in mind that you are participating in a class. Something that would be inappropriate in a traditional classroom is also inappropriate in an online classroom.

Online Communication:

- Be careful with humour and sarcasm. Both can easily be misunderstood!
- Review all discussion postings before posting your own to prevent repetition.
- Stay on the topic which has been identified in the initial post or heading.
- Check your writing for errors by reviewing what you've written before submitting it.
- Do not use abbreviations or acronyms eg BBL (Be Back Later) as many users may not know what you mean or misinterpret your comment.
- No matter what forum, writing in all capital letters is considered SHOUTING and is considered very rude. A word or two in caps is fine, but shouting is not recommended.
- Obey copyright laws. Don't post material in a workspace or as an attachment in a discussion forum without acknowledging the source e.g. This picture was downloaded from

Source: www.thinkuknow.com

Information for Pupils

Information on the risks associated with social networking sites including advice on how to avoid the risks and enjoy using these sites.

Quick tips on how to protect your mobile devices.

Detailed information on how to protect your mobile devices.

Information on the sexting, protecting yourself, the law.

How to stay in control and what to do if an image falls into the wrong hands.

Information about keeping safe online, run by the Safeguarding Board for Northern Ireland.

E-Safety Advice for Parents/Carers

1. Talk to your child about the benefits and risks of internet use so that you can help educate them to use the internet safely.

2. Develop an interest in your child's online activities, including favourite websites, online games and interests, and be aware of what your child is doing online.

3. Be aware of your child's use of social media.

4. Ask your child who he/she is talking to online and remind them how important it is to tell a trusted adult if something happens online that makes them feel uncomfortable or worried.

5. Be aware of the advice and information available relating to e-safety. Websites containing advice for parents/carers and children include:

www.ceop.police.uk

www.childline.org.uk

www.getsafeonline.org

www.internetmatters.org

www.nspcc.org.uk

www.net-aware.org.uk/#

www.saferinternet.org.uk

www.thinkuknow.co.uk

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