Victoria College Belfast

E-Safety Policy

Policy Date – June 2023

Review Date –

Governor approval – 12.06.23

Drafted by – M Gray

1. Rationale

Digital Technology has become an integral part of the lives of pupils in today's society. Digital Technology and the online world have opened a range of opportunities for pupils and have the potential to add value to pupils' education. However, alongside this, there is a growing concern about the negative impact that these technologies could potentially have if not used safely.

As a College we need to be progressive about our response to the ever-increasing reliance on Digital Technology and the changes it brings to our society.

At Victoria College Belfast. we believe that there are significant benefits that come from learning, exploring and connecting with each other online. We also know how important it is to make sure pupils know how to protect themselves. Victoria College Belfast is committed to raising awareness of the potential risks pupils face online and how these concerns can be reported. The College will ensure each pupil is educated about how to act appropriately online and stay safe.

The potential risks pupils may encounter online are broadly grouped into 4 categories, due to the rapidly evolving nature of E-Safety and development of new technologies.

1. Conduct

A Pupil may be at risk because of their own behaviour, for example, by sharing too much information.
Some of the conduct risks pupils may face include:

- The potential for excessive use which may impact on the social and emotional development and learning of the pupil.
- Plagiarism and copyright infringement.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Digital footprint and online reputation.
- Sexting.

2. Content

Age-inappropriate or unreliable content can be available to pupils.
Some of the content risks pupils may face include:

- Exposure to inappropriate content, including online pornography and violence.
- Access to illegal, harmful or inappropriate images or other content.
- Lifestyle websites, for example eating disorders, self-harm or suicide sites.
- Hate sites.
- Access to unsuitable video / internet games.
- Content validation: an inability to evaluate the quality, accuracy and relevance of information on the internet.

3. Contact

Pupils can be contacted by bullies or people who groom or seek to abuse them.
Some of the contact risks pupils face may include:

- Inappropriate communication / contact with others, including strangers.
- The risk of being subject to grooming.
- Cyber-bullying.
- Identity theft and sharing passwords.

4. Commercialism

Pupils can be unaware of hidden costs and advertising in games, apps and websites. Some of the commercial risks pupils may face include:

- Pop-ups and spam emails.
- In-app purchasing.
- Advertising.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore our aim, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

Every School must demonstrate that it has provided the necessary safeguards, to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-Safety Policy that follows explains how Victoria College Belfast intends to help pupils be responsible users and to stay safe, while using the internet and other communication technologies for educational, personal and recreational use.

Scope

For the purpose of common understanding, this policy assumes the following definition of e-safety:

"E-Safety is about using electronic devices in a safe, responsible and respectful way. It means safeguarding children and pupils in the digital world and educating them to keep themselves safe online".

NI Executive E-Safety strategy and policy for NI 2019-2022

Pupils are expected to behave online in a way that does not compromise their own safety, the safety of others or the reputation of the College. All staff and pupils are expected to adhere to this e-safety policy and this policy should be used in conjunction with our Anti-Bullying, Acceptable Use and Safeguarding & Child Protection Policies.

In relation to incidents that occur during College hours, we will work with parents/guardians/guardians, staff and pupils to ensure the e-safety of all involved, and, if necessary, to apply sanctions as per our Positive Behaviour, Anti-Bullying and Child Protection Policies as appropriate.

In relation to e-safety incidents that occur outside of College hours, the College will work with pupils and parents/guardians to help keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents/guardians. If inappropriate activity occurs outside school hours, resulting in a negative effect on any member of the School community, and it is brought to our attention, then we will consider our response alongside the Anti-Bullying, Positive Behaviour and Child Protection and Safeguarding policies.

2. Roles and Responsibilities

Board of Governors

The Board of Governors has a duty to safeguard and promote the welfare of pupils and to determine the measures to be taken by the College to protect pupils from online abuse. In exercise of these duties, the Governors must ensure that an E-Safety Policy has been approved and implemented. Oversight of the operation of this policy will be through the Curriculum Committee.

The Principal

The Principal will:

- Have overall responsibility for e-safety.
- Support the Safeguarding Team and ICT Co-ordinator in the development of an online safety culture within the College.

Vice-Principal (Pastoral)

The Vice-Principal (pastoral) will be the Designated Teacher for E-Safety and will:

- Act as a named point of contact on all online safety issues and liaise with other members of staff and agencies as appropriate.
- Keep up to date with current research, legislation and trends and adjust policy and practice accordingly.
- Coordinate participation in events to promote positive online behaviour, e.g., Safer Internet Day.
- Ensure that online safety is promoted to parents/guardians/carers and the wider community through a variety of channels and approaches.
- Maintain an online safety incident/action log to record incidents and actions taken as part of the College's safeguarding recording structures and mechanisms.
- Monitor the College's online safety incidents to identify gaps/trends and adjust policy and practice accordingly, and report to the Principal as appropriate.
- Ensure that online safety is integrated with other appropriate College policies, procedures and guidelines.
- Ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety and provide guidance regarding safe, appropriate communications.
- Ensure that suitable, age-appropriate and relevant filtering is in place to protect pupils from inappropriate content to meet the needs of the College and ensure that the filtering and system is actively monitored.
- Work with and support technical staff in monitoring the safety and security of the College's systems and network.

The Designated Teacher may delegate some aspects of the responsibilities listed above to members of the wider Pastoral Team (Senior Teacher, Heads of Year, Form Tutors), as appropriate.

Whole College ICT Co-ordinator

The ICT Co-ordinator will:

- Liaise with the Vice-Principal (pastoral) to explore ways of promoting e-safety to pupils, parents/guardians and staff.
- Liaise with the Vice-Principal (pastoral) to coordinate participation in events to promote positive online behaviour, e.g., Safer Internet Day.
- Keep up to date with current research, legislation and trends and adjust policy and practice accordingly.
- Contribute to the development of E-Safety Policies.
- Work with the Head of Digital Technology to deliver an ICT curriculum which promotes age-appropriate online safety messages for students on how to stay safe and how to take responsibility for their own and others' safety.
- Attend and disseminate relevant CPD to staff of the College.

ICT Technician

The ICT Technician will:

- Ensure that the use of the College's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the Designated Teacher for e-safety.
- Regularly monitor the use of the network and report any breaches or concerns to the Designated Teacher for e-safety and together ensure that they are recorded, and appropriate action is taken.

Staff

Teaching and non-teaching staff will:

- Contribute to the development of E-Safety Policies and procedures.
- Adhere to the College E-Safety Policy and Acceptable Use Policies (Appendix 1)
- Sign and return the Agreement Form appended to any relevant Acceptable Use Policy.
- Have an awareness of e-safety matters and how they relate to pupils.
- Model good practice in using new and emerging technologies.
- Embed e-safety education in curriculum delivery where possible.
- Report any concerns to the Designated Teacher for E-Safety.
- At all times adhere to the College Code of Conduct for Staff and Volunteers.

A list of Acceptable use of various technologies for staff and pupils can be found in Appendix 2

Pupils

Pupils will:

- Contribute to the development of E-Safety Policies and procedures.
- Read the College's E-Safety Policy and Acceptable Use Policies and adhere to them.
- Sign and return the Agreement Form appended to any relevant Acceptable Use Policy.

- Seek help from a trusted adult if things go wrong and offer support to others that may be experiencing online safety issues.
- Take responsibility for keeping themselves safe online.
- Take responsibility for improving their awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assess their personal risk of using any technology and behave safely and responsibly to limit those risks.
- In circumstances where pupils have been given permission to bring their own device to College, they must read and sign the BYOD policy (Appendix 3).

A list of Acceptable use of various technologies for staff and pupils can be found in Appendix 2 with possible sanctions in Appendix 4.

Parents/guardians

Parents/guardians should:

- Understand the College's E-Safety Policy, Acceptable Use Policies and encourage their child/children to adhere to them.
- Read and submit consent to any relevant Acceptable Use Policy.
- Read all information regarding e-safety shared with them by College.
- Support the College in their e-safety approaches and reinforce appropriate safe online behaviour at home.
- Model safe and appropriate uses of new and emerging technology.
- Additional guidelines for parents/guardians can be found in appendix 5.

3. Communication of e-safety

3.1 Policy access

This policy is available, on request, from the College Reception and on the College website

3.2 Professional development for 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:

- E-safety information will be made available to new staff as part of their induction. Where necessary training and e-safety updates will also be provided during the academic year.
- All new staff should receive e-safety information as part of their induction programme, ensuring that they fully understand the College E-Safety and Acceptable Use Policies.

3.3 Education of pupils

The education of pupils in e-safety is an integral part of the College's provision allowing pupils to recognise and avoid e-safety risks and to build their resilience. E-safety is promoted through, but not limited to:

- Specific ICT lessons.
- ICT across the curriculum.
- Talks from external agencies (e.g., PSNI).
- Personal Development lessons delivered through the LLW and Form Time curriculum.
- Assembly.
- Safer Internet Day.
- Anti-bullying week.

There are also various resources available at:

- Know it all Colleges
  https://www.childnet.com/resources/kia/know-it-all-secondary-toolkits

- Think you know
  https://www.thinkuknow.co.uk/

- Childnet
  https://www.childnet.com/sorted/

3.4 Education of Parents/Guardians

The College recognises that parents/guardians have an essential role to play in enabling their daughter(s) to become safe and responsible users of the internet and digital technology. Parents/guardians' attention will be drawn to the College's Policy and expectations. Information and guidance for parents/guardians on online safety will be made available in a variety of formats, e.g. emails, VCB social media pages. Parents/guardians will be encouraged to model positive behaviour for their daughter(s) online.

Parents/guardians are strongly encouraged to have regular conversations with their child) about the benefits and dangers of the Internet, to empower them to use the Internet safely. More advice can be found at the end of this policy in Appendix 5.

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- https://www.familylives.org.uk/advice/your-family/online-safety/internet-safety/
  Aimed at parents/guardians and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
- http://www.bbc.co.uk/webwise/a-z/
  Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- https://www.ceop.police.uk/safety-centre/
- The government's Child Exploitation and Online Protection Centre (CEOP) Safer internet NI App. Parent can download and install the app from the relevant app store on their smartphone.

3.5 Managing emerging technologies

There is an ever-increasing reliance on Digital Technology, and as a College, we aim to be progressive about our response to changes Digital Technology brings to our society. The College risk-assess any new technologies before they are allowed in School and consider any educational benefits that they may have. The School keeps up to date with new technologies and will quickly develop appropriate strategies for dealing with new technological developments and any associated risks.

4. Cyber bullying

For common understanding, this Policy assumes the following definition of cyberbullying:

"Cyber bullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else".

UK Safer Internet website

Staff should be aware that pupils are vulnerable to cyberbullying both in and out of College. This form of bullying is considered within the College's Ant-Bullying Policy as well as in this E-Safety Policy.

The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. However, most messages can be traced back to their creator. Although there is no specific legislation for cyberbullying, the following may cover different elements of cyberbullying 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

Offensive material relating to the College, or any member of the school community, should not be posted online, regardless of whether this has been done at School or another place.

- All instances of cyberbullying are forbidden and will be dealt with according to the College's Anti-Bullying Policy.
- If pupils think they are being bullied online, they should speak to a member of staff or a parent/guardian as soon as possible.
- If staff feel that they are abused online, they should speak to a member of SLT as soon as possible.

Mobile Phones

The College recognises that many parents/guardians may wish their daughter to have a mobile phone for use in cases of emergency. However, mobile phones can be used inappropriately, and they are potential targets for theft and online bullying-type behaviour. The College reserves the right to confiscate a pupil's mobile phone and retain it at Reception until 3.10 pm, should a pupil fail to co-operate with the arrangements outlined below. They will then have an appropriate sanction issued in accordance with the Positive Behaviour Policy.

The use of mobile phones is restricted and must be SWITCHED OFF AT ALL OTHER TIMES, including between classes, unless directed otherwise by staff.

The misuse of mobile phones and other personal electronic communication equipment for online bullying-type behaviour will not be tolerated (see Anti-Bullying, Positive Behaviour, Internet Acceptable Use and Social Media Policies).

In class, pupils may use their mobile phones if directed to do so by their teacher. There are colour coded signs placed in classrooms and corridors which indicate if pupils are allowed to use their phones:

Red: pupils are not permitted to use their phone.

Orange: pupils are permitted to use their phone only when allowed by a staff member.

Guidelines have been shared with staff and pupils for the expectations and acceptable use of phones in VCB (see Appendix 6 and 7)

5. Published content

5.1 College Website

The contact details on the website will be the College address, email and telephone number. Staff or pupils' personal information will not be published. While the Principal may delegate the day-to-day operation of the website, the Principal will take overall editorial responsibility for online content published by the School will ensure that content published is accurate and appropriate. The School website will comply with the School's current guidelines for publications including use of pupils' images, respect for intellectual property rights, privacy policies and copyright.

5.2 Publishing images and videos online

Use of images and video is an increasingly important element in modern educational practice. Videos can be produced by staff or pupils for a variety of educational purposes as well as for promotion and recording of activities.
Images and videos may in some circumstances be published to an external storage or video sharing website. Where this is the case, current guidelines on the use of these facilities will be followed by pupils and staff.
The College will ensure that permission from parents/guardians has been obtained via the SIMS parent app before images/videos of pupils are electronically published.

5.3 Managing Email

The College will provide all pupils and staff with at least one official email address. These addresses are the only ones which should be used for school communication and educational purposes.

Pupils and staff will be made aware of the appropriate use of email and the sanctions if they abuse the email system. They will also be advised to be careful regarding with whom they share this email address. Pupils will be advised that this email address should only be used for College related activities and that it is not private.

These addresses may be used to allow pupils to access services which the College has sanctioned, as appropriate, for use within College, cloud-based storage and associated applications). Use of email accounts and any services accessed using that account will only be used in accordance with the current school guidelines

5.4 Official College Use of Social Media

Official social media used by the College will be in line with existing policies, including Anti-Bullying, Safeguarding and Child Protection. Images or videos of pupils will only be shared on official College media sites/channels in line with the guidelines on image use which can be found in our Safeguarding and Child Protection Policy.

Social media use will be age appropriate. The College is aware that many social media sites state that they are not for children under the age of 13, therefore the College will not create accounts within College for pupils under this age.

Information about safe and responsible use of College social media channels will be communicated clearly and regularly to all members of the College community The Principal and Designated Teacher for e-safety must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence. Parents/guardians and pupils will be informed of any official College use, along with expectations for safe use and School actions to safeguard the community.

Where social media is used as part of a lesson or other educational experience this will be under the control of a member of staff. Staff discretion is advised and should be in line with the current guidelines and the Staff Code of Conduct.

Official use of social media sites by the College will only take place with clear educational or engagement objectives with specific intended outcomes e.g., revision forums or increasing parental engagement. Staff use of social media sites as communication tools will only be used with permission of the Principal. College media channels will be set up as distinct and dedicated social media site or accounts.

College social media accounts will be sanctioned by the Principal and will be set-up and managed by a member of College.

Staff will use College provided email addresses to register for, and manage, official College social media channels. Members of staff running official College Social Media channels must ensure that they obtain prior permission from the Principal/Vice-Principals, are aware of the required behaviour and expectations of use and will monitor the use of the channel(s) to check they are being used safely, responsibly and in accordance with local and national guidance and legislation.

All communication on official College social media platforms will be clear, transparent and open to scrutiny. Any online publication on official College media sites will comply with legal requirements including GDPR, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information, and will not breach any common law duty of confidentiality or copyright.

Staff will not engage with any direct or private messaging with pupils or parents/guardians through Private social media accounts and should communicate via recognised College communication channels.

Any concerns regarding the online conduct of pupils, parents/guardians, or staff on social media sites should be reported to the Designated Teacher for E-safety or Designated Teacher for Child Protection and will be managed in accordance with existing College policies such as Anti-Bullying, Staff Code of Conduct, Safeguarding and Child Protection.

6. Management of systems

6.1 Data security

Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulations (GDPR).

All users will be informed not to share passwords with others and not to login as another user at any time. Staff and pupils must always keep their passwords private and must not share them with others or leave it where others can find them. All members of staff will have their own unique username and private passwords to access College systems. Members of staff are responsible for keeping their passwords private.

6.2 Filtering

The College uses a filtered Internet and email service provided by C2K. The system is designed to filter sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.

If a member of staff or pupil should unwittingly discover an unsuitable site, the URL should be reported to the ICT Support Officer or the Designated Teacher for e-safety. This will then be recorded and escalated as appropriate to C2K.

Any deliberate access to prohibited/unsuitable sites (within College or using a College device) will be dealt with, as appropriate, according to the School's College Pupil Positive Behaviour/Code of Conduct for Staff and Volunteers.

6.3 Applications and Software used to Record Pupil Information

The Principal is ultimately responsible for the security of any data or images held of pupils. Apps/systems which store personal data will be assessed prior to use. Only College issued or sanctioned devices will be used for apps that record and store pupils' personal details, attainment or photographs.

Devices will be appropriately protected if taken off site to prevent a data security breach in the event of loss or theft.

7. Policy Review

This policy will be reviewed every three years from the date it is approved by the Board of Governors.

8. Associated Policies

The following policies/other College documents are associated with this E-Safety Policy:

- Acceptable Use of the Internet.
- Anti-Bullying Policy.
- Positive Behaviour Policy.
- Safeguarding and Child Protection Policy.
- AUP for C2K managed portable devices.
- VCB Surface Pro AUP
- Code of Conduct for Staff and Volunteers.
- Conditions for Using Images of Pupils, Consent Form.

Appendices

Appendix 1

AUP C2K managed devices

EN094 Acceptable
Use Policy for C2K Ma

Appendix 2: Acceptable use of various technologies for staff and pupils.

	Staff and Other adults				Students/Parents/Guardians			
Communication technologies	Allowed	Allowed at certain times	Allowed for selected staff*	Not allowed	Allowed	Allowed at certain times	Allowed for selected pupils/parents/gu	Not allowed
Mobile phones brought to College	✓	✓			✓			
Mobile phones used in lessons	✓					✓		
Taking photos/videos/ recordings on mobile phones or other camera devices of lesson content	✓					✓		
Taking photos/videos/ recordings on mobile phones or other camera devices of other teachers/pupils			✓					✓
Use of other devices e.g. laptop/ tablet/ ipad to support T&L	✓					✓		
Use of personal email addresses in College, or on College				✓				✓
Use of College email for personal emails				✓				✓
Use of chat rooms / facilities		✓						✓
File sharing websites				✓				✓
Use of social networking sites			✓					✓
Online Shopping on College device				✓				✓
Online gaming (educational)		✓				✓		
Online gaming (non - educational)				✓				✓
Cloud based storage linked to school accounts	✓				✓			

Cloud based storage linked to personal accounts				✓				✓

***Permission must be sought and approved by the Principal/Vice Principal before use.**

Appendix 3

BYOD Consent

BYD consent.docx

Appendix 4 Sanctions for inappropriate/harmful/misuse of ICT in College or relating to College

Incident:	Verbal reprimand	Behaviour Point	Referral to HoY/HoS	Wednesday detention	Referral to senior staff	Internal suspension	Suspension	Expulsion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓	✓					
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of social networking / instant messaging / personal email	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓	✓				
Allowing others to access College network by sharing username and passwords	✓	✓	✓					
Attempting to access or accessing the College network, using another student's / pupil'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 instant 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 Data Protection Act				✓	✓	✓	✓	✓

Appendix 5

Additional Advice for Parents/guardians with Internet Access at home

1. A home computer with Internet access should be situated in a location where parents/guardians can monitor access to the Internet.

2. Parents/guardians should agree with their children suitable days/times for accessing the Internet.

3. Parents/guardians should discuss with their children the College rules for using the Internet and implement these at home. Parents/guardians and children should decide together when, how long and what constitutes appropriate use;

4. Parents/guardians should get to know the sites their children visit and talk to them about what they are learning;

5. Parents/guardians should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents/guardians' Information Network (address below);

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

7. Parents/guardians should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the College name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents/guardians should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the College they should immediately inform the College

Appendix 6

Teacher guidelines for mobile phone usage

teacher guidlines
mobile phones.docx

Appendix 7

Mobile phones for learning- pupil poster

mobile phones for
learning pupil poster.