Cookstown High School

Online Safety Policy

Reviewed: December 2024

Next Review: December 2025

Contents

POLICY OVERVIEW

DETAILS

TITLE	Online Safety Policy
TARGET AUDIENCE	Governors', Staff, Parents/Carers
REVIEW DATE	December 2024
REVIEW LEAD	Principal
POLICY DEVELOPED BY	Senior Leadership Team
POLICY RATIFIED BY THE BOARD OF GOVERNORS:	December 2024
EFFECTIVE FROM:	December 2024
REVIEW FREQUENCY:	Every year
REVIEW DATE:	December 2025
PRINCIPAL	Miss G J Evans
CHAIR OF BOARD OF GOVERNORS	Mrs L Dripps

RECORD OF POLICY AMENDMENTS

The following table outlines any significant changes/amendments made to this procedure since it was ratified by the Board of Governors on:

DATE OF REVIEW OR AMENDMENT	SUMMARY OF CHANGED / AMENDMENTS TO PROCEDURE	AMENDED BY

Rationale

Cookstown High School is committed to safeguarding and promoting the welfare of pupils in an increasingly digital world. This policy outlines safe, acceptable, and effective use of online resources and digital tools, with a primary focus on safeguarding all users within the school community.

All members of staff and the Board of Governors of Cookstown High School have a responsibility to safeguard and promote the welfare of pupils. This policy promotes safe, healthy, acceptable, and effective use of the Internet and other digital tools in school. Furthermore, this policy outlines safe and acceptable working practices for all staff and pupils, ensuring a primary emphasis on safeguarding and welfare of all who use online facilities at Cookstown High School.

Linked documents:

- Bring Your Own Device (BYOD) Policy
- Safeguarding & Child Protection and Policy
- Positive Behaviour Policy
- Addressing Bullying Policy

Mission Statement

As a school founded upon Christian principles, we believe in and celebrate the uniqueness of each individual and encourage all members of our community to show respect for all.

We seek the development of Character through Knowledge believing each individual has a duty to build a community, to strive to do their best, to show compassion for those in need, and to take responsibility for their own words and actions.

Cookstown High School seeks to develop young people who are independent learners and active citizens.

C2K and MySchool Services

All schools in Northern Ireland have been provided with access to the Internet, email and online conferencing through Classroom 2000 (C2K). This ensures provision of hardware, software and connectivity for Northern Ireland schools. Wi-Fi throughout the school provides a wider connectivity range to classrooms and areas of learning within the school.

MySchool provides a range of learning tools, resources and apps for use in teaching and learning across all subject areas. An expanding aspect of this area is the Virtual Learning Environment (VLE) which allows remote teaching and learning to continue through programs such as Google Classroom and Office 365.

C2K provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Some of these safety services include:

- Providing all users with a unique username and password
- Tracking and recording all online activity
- Scanning all C2K email and attachments for inappropriate content and viruses.
- Appling a filter to websites and emails
- Providing appropriate curriculum software

If additional service providers other than C2K are required, effective firewalls, filtering and software

monitoring mechanisms will be put in place by the school and C2K.

Securus is an e-monitoring application that adds additional levels of filtering and monitoring of network-based activity. Instances of misuse of school technology will be detected across a range of specified areas, including:

- Attempting to bypass security or access restricted sites
- Use of inappropriate language
- Activities related to Cyberbullying

Codes of Safe Practice

When using the internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination, and obscenity.

No network or internet user is permitted to:

- Retrieve, send, copy or display offensive messages or pictures
- Use obscene or racist language
- Harass, insult or attack others
- Damage computer systems or networks
- Violate copyright laws
- Use another user's password
- Trespass in another user's folders, work, or files
- Intentionally waste resources (such as consumables, bandwidth); Use the network for unapproved purposes
- Pass security systems, including unauthorised use of artificial intelligence tools for prohibited activities

The scope of the codes of practice applies to all forms of e-technology within the school: school PCs, iMacs, laptops, iPads and any digital video or photographic equipment. Any devices not owned by the school but brought on to school premises by pupils or staff (such as mobile phones, laptops) are subject to the same requirements as technology provided by the school.

The codes of practice will be monitored and updated in line with continuing developments in ICT across the school.

The school will ensure that access to the Internet is through a reputable Internet Service Provider (ISP) and that this is a filtered service. Machines which are connected to the Internet will be in full view of people circulating in the area. Pupils engaged in research or internet-based learning must be in supervision of a member of staff.

Code of Safe Practice for Pupils

Pupils are responsible for their good behaviour on the school networks; access to ICT provision remains an integral part of teaching and learning, and pupils who breach the Code of Safe Practice will be punished in line with the school's Positive Behaviour Policy.

The Code of Safe Practice for Pupils will be displayed prominently in classrooms. The use of mobile phones by pupils is not permitted on the school premises from 9:25 to 3:55pm, as set out in the homework diary, unless directed by the subject teacher for educational purposes. Online activities which are encouraged include:

- Use of email and computer conferencing for educational purposes
- Use of the internet to investigate and research school related work

- Use of the internet to research careers and Further and Higher education opportunities
- Use of the school's VLE
- Completion of UCAS applications

While the Code of Safe Practice for pupils is designed to be rigorous, it cannot be 100% effective at all times. Neither the school nor C2K can accept liability under such circumstances.

Incidents of misuse which arise will be dealt with in accordance with the schools' Positive Behaviour Policy. Minor incidents will be dealt with by the class teacher/Head of Year and may result in a temporary ban on internet use. Incidents involving child protection and safeguarding will be dealt with in accordance with the school's Child Protection and Safeguarding Policy.

The Code of Safe Practice for pupils is in Appendix 1 of this document.

Code of Safe Practice for Staff

All staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector. Staff are expected to observe the Code of Conduct in all online communications.

The Code of Safe Practice for Staff serves to monitor use by pupils, ensure safe and appropriate use of the internet and to protect all users through consistently effective and careful use.

While normal privacy is respected and protected by password controls, users must not expect files stored on servers to be absolutely private: user areas may be inspected from time to time.

The following standards should be adhered to:

- Pupils using the internet should be supervised by a member of staff at all times
- Staff will make pupils aware of the Code of Safe Practice for pupils
- Any pupils found to be in breach of the Code of Safe Practice will be reported immediately to the Vice-Principal (Pastoral)
- Staff passwords should only be shared with the Network Manager
- Be aware of copyright and intellectual property rights and be careful not to download materials which would be in breach of these rights
- Photographs of pupils should be taken on a school camera or school provided iPad and stored on the school network, accessible only to staff
- School systems may not be used for commercial transactions

A more detailed Code of Safe Practice for staff is available in Appendix 2.

Online activities not permitted by any user include:

- Searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- Copying, saving and/or redistributing copyright protected or offensive material;
- Subscribing to any services or ordering any goods or services, unless specifically approved by the school;
- Playing computer games or using interactive 'chat' sites, unless specifically assigned by the teacher;
- Using the network in such a way as to disrupt other users (e.g. downloading large files during peak usage times, sending mass email messages);
- Publishing, sharing or distributing any personal information about a user (e.g. home address, email address, phone number);

- Altering or attempting to alter the system in any manner not specifically approved by the school (e.g. hacking, installing viruses etc.); Any activity that violates a school rule.

Internet Safety Awareness

Education of safe use of the internet is essential, as all members of the school community benefit from the array of resources available through C2K. Promoting Internet Safety Awareness is as important for staff and parents as it is for pupils, and training, information and special events help to maintain an ongoing focus on acceptable internet use.

There are various resources available for parents, staff and pupils to access:
http://thinkuknow.co.uk http://bbc.co.uk/webwise
http://kidsmart.org.uk
http://careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
http://www.parentscentre.gov.uk/usingcomputersandtheinternet
http://ceop.gov.uk
https://onlinesafetyhub.safeguardingni.org/
https://onlinesafetyhub.safeguardingni.org/young-people/

Mobile Phone Usage

Pupils are prohibited from using personal mobile phones during school hours unless specifically permitted for educational purposes by a teacher.

Privacy and Safety Settings

Staff will complete EA provided Cyber Security Training on an annual basis.
https://staffhub.eani.org.uk/hr-online/statutory-and-mandatory-training/school-managed-staff-statutory-and-mandatory-training-1

Pupils will be encouraged to update privacy settings on personal devices and understanding the importance of protecting personal data online.

A checklist for Privacy and Safety Setting is included in Appendix 2

Health and Safety

Maintaining a safe working environment at all times is essential to ensure effective learning and teaching space for all. ICT rooms are well laid out, and pupils are supervised at all times. Digital projectors, interactive whiteboards and portable forms of digital technology are maintained within departments and issues with Health and Safety should be reported to the V-P (Curriculum). Parents of pupils who may have a physical reaction to screens or require seating in a particular part of a room, should inform the Vice-Principal (Pastoral).

Staff and pupils will be encouraged to manage their screen time effectively, ensuring regular breaks from digital devices.

Activities to promote digital wellbeing and discussions on healthy online habits will be encouraged.

The School Website/Social Media

The school website / Social Media is used to provide information, promote the school and celebrate the success of our pupils. Editorial supervision will ensure that content reflects the school's ethos, and that personal security is not compromised. The school website/social media safeguards the interests of pupils and staff by:

- Providing the school address, school email and telephone number as the point of contact. Staff or pupils' home information will not be published
- Photographs that include pupils will be selected carefully, will limit personal information provided
- Pupils' full names will not be used anywhere on the school's website, particularly in association with photographs
- The Principal or website manager will take editorial responsibility and ensure that content is accurate and appropriate
- The web site should comply with the school's guidelines for publications
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained

Social Software and Filtering

C2K filtering happens at different levels and allows or blocks access to a variety of web sites and resources online. Filtering is grouped as follows:

- Internet advanced – allowing access to a wider range of pages than the default including webmail, shopping, drugs and alcohol, sex education
- Internet streaming – allowing access to streaming media websites including YouTube, BBC iPlayer, Vimeo, TV and radio streaming sites
- Internet Social Networking – allowing access to social networking sites including Facebook, Twitter, LinkedIn, Wordpress

Through the managed service provided, standard security includes:

- Forcepoint (formally Websense) filtering in place for internet access
- Nightly Internet Watch Foundation (IWF) updates
- All staff and pupil internal and external email is filtered for inappropriate content

Cyberbullying

Instances of cyber bullying of pupils or staff will be regarded as a very serious offence and dealt with according to the school's Positive Behaviour Policy and Child Protection and Safeguarding Policy.

Advice for Parents

Appropriate use of the internet continues at home, where schoolwork and study can benefit from the wealth of resources available. The school advises parents to provide filtered and supervised use of the internet at home, and the following guidance is provided:

- Discuss with your child the rules for using the internet and decide together when it should be used, for how long and for what purposes
- Get to know the sites your child is visiting, and talk with them about what they are learning
- Ensure that you give agreement before your child gives out any personal information on the internet, such as a picture, an address, a phone number, the school name or financial details

- Encourage your child to avoid responding to any unwelcome, unpleasant or abusive messages, and to tell you if they receive any such messages. If this type of message is received through a connection provided by school or Learning NI, the school must be informed immediately

Advice for parents/guardians is freely available from:

NCH Northern Ireland
45 Malone Road
Belfast BT9 6RX Tel:
028 9068 7785
http://www.nchafc.org.uk/ITOK

Child Exploitation and Online Protection Centre
33 Vauxhall Bridge Road
London SW1 2WG Tel:
0870 000 3344
http://www.ceop.police.uk
https://onlinesafetyhub.safeguardingni.org/

Appendix 1

Code of Safe Practice (Pupils)

- I will only use ICT systems in school, including the internet, email, or any other mobile technology, for school purposes.
- I will not download or install software on school equipment.
- I will only log-on with my own username and password
- I will follow the school's ICT security system and not reveal my password to anyone. I will change my password regularly.
- I will only use my school email address.
- I will make sure that all ICT communication with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/or staff will only be taken, sorted, and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Principal.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technology can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/guardian will be contacted

Appendix 2

Code of Safe Practice (Staff)

ICT and related technologies are an expected part of our everyday working life. Email, the internet and mobiles devices are an integral part of our work. This code of practice is designed to ensure that all staff are aware of their professional responsibility when using any form of ICT. All staff are expected to always adhere to the contents below. Any concerns or clarification should be discussed with the principal.

- I will only use the school's email, internet, intranet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number and personal email address to pupils.
- I will only use the approved C2K secure email system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
- I will not install hardware or software without permission of the ICT Co-Ordinator.
- I will not browse, download, upload, or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupil and/or staff will only be taken, stored, and used for professional purposes in line with school policy and with written consent of the parent, carer, or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or the Principal.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available on request to my line manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety and GDPR security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- Ensure responsible use of AI and other emerging technologies in lesson planning and assessments.

Appendix 3

Privacy and Safety Settings Checklist

This checklist is designed to support pupils and staff in understanding and applying best practices for online privacy and safety. It should be used during workshops and as a reference for safe online behaviour.

General Privacy Practices

Update Passwords Regularly

- Use strong, unique passwords for each account.
- Include a mix of letters, numbers, and special characters.
- Change passwords every 3-6 months.

Enable Two-Factor Authentication (2FA)

- Activate 2FA for all accounts to add an extra layer of security.

Review Account Privacy Settings

- Regularly check and update privacy settings on all social media and online accounts.
- Restrict who can view your profile, posts, and contact information.

Keep Personal Information Private

- Avoid sharing sensitive details such as home addresses, phone numbers, or financial information online.

Safe Online Behaviour

Be Cautious with Links

- Avoid clicking on links from unknown or untrusted sources.
- Verify URLs before entering personal information.

Think Before Sharing

- Consider the audience and potential consequences before posting or sharing anything online.

Recognise Phishing Attempts

- Be wary of emails or messages requesting personal information.
- Look for signs of phishing, such as poor grammar or urgent requests.

Avoid Public Wi-Fi for Sensitive Tasks

- Refrain from logging into accounts or conducting financial transactions over public Wi-Fi unless using a VPN.

Device Security

Install Security Updates

- Regularly update devices and software to patch vulnerabilities.

Use Antivirus Software

- Install and maintain reliable antivirus and anti-malware programmes.

Monitor App Permissions

- Review and limit app permissions to access only necessary data.

Secure Devices

- Lock devices with passwords, PINs, or biometric security when not in use.

Social Media Safety

Limit Location Sharing

- Disable location sharing unless absolutely necessary.

Review Tagged Content

- Check and approve tags before they appear on your profile.

Manage Friend Requests Carefully

- Only accept friend requests from people you know personally.

Be Aware of Digital Footprint

- Remember that anything shared online can be permanent, even if deleted.

Regular Reviews

Audit Online Accounts

- Periodically review and delete unused accounts.

Check Privacy Policies

- Familiarise yourself with the privacy policies of frequently used apps and websites.

Educate and Stay Updated

- Attend workshops and stay informed about the latest online safety trends and threats.

Report Issues

- Immediately report suspicious activities or breaches to the school's ICT team or a trusted adult.