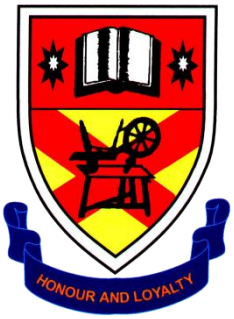
CLOUNAGH JUNIOR HIGH SCHOOL

ONLINE SAFETY POLICY

Revised January 2019

CONTENTS



1. Rationale

All members of staff and the Board of Governors of Clounagh JHS 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. This policy is constructed on the advice stated in Circular 2016/27 on Online Safety by the Department of Education. 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 Clounagh JHS.

Linked documents:

- Safe Guarding & Child Protection Policy
- Behaviour Management Policy

2. 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 Fronter and Google Classroom.

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 user name and password
- Tracking and recording all online activity
- Scanning all C2K email and attachments for inappropriate content and viruses.
- Applying a filter to websites and emails
- Providing appropriate curriculum software

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

3. 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 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.

The scope of the codes of practice applies to all forms of e-technology within the school e.g. school PCs, iPads. 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.

3.1 Code of Safe Practice for Pupils (Appendix 1)

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 will be punished in line with the school's Behaviour Management Policy when rules are breached. Pupils engaged in research or internet based learning must be in supervision of a member of staff.

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.

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' Behaviour Management 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 Safe Guarding & Child Protection Policy.

3.2 Code of Safe Practice for Staff (Appendix 2)
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 ICT Technician;
- 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;
- Searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers.

Online activities not permitted by any user include:

- 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.

4. 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

5. 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 V-P (Pastoral).

6. The School Website and Facebook Page

The school website and facebook page 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 and facebook page 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 limited personal information provided;
- Pupils' full names will not be used anywhere, particularly in association with photographs;
- The Principal or website manager will take editorial responsibility and ensure that content is accurate and appropriate;
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7. 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 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

8. 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 Behaviour Management Policy and Safe Guarding & Child Protection Policy.

9. Advice for parents

Appropriate use of the internet continues at home, where school work and study can benefit from the wealth of resources available. The school advices 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, 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

10. Incident Reporting, Online Incident log and Infringements

10.1 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Coordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your eSafety co-ordinator.

10.2 E-Safety Incident Log

Details of all eSafety incidents to be recorded by the eSafety Coordinator. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

Date & Time	Pupil / Staff Name	Room and computer/ device number	Details of Incident	Action and Reasons

10.3 Misuse and Infringements

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by Clounagh JHS.

10.4 Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Principal.

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 user name 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

Dear Parent/Guardian,

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or guardian and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Mr G Eakin - eSafety co-ordinator.

Please return the bottom section of this form to school for filing.

Pupil and Parent/ Guardian signature

We have discussed this document and ……..(pupil name) agrees to follow the Code of Safe Practice (Pupils) and to support the safe and responsible use of ICT at Clounagh JHS.

Parent/ Guardian Signature ……

Pupil Signature…….

Class ……. Date ……

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 adhere at all time 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 Online Safety and GDPR security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

Staff Name:…….

Staff Signature:…….

Date:……