BALLYCASTLE HIGH SCHOOL

E-Safety Policy

- *Approval by the Board of Governors:* ***Updated Nov 2018***
- *The implementation of this policy will be monitored by: Senior Management Team*
- *This policy will be reviewed annually*

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Ballycastle High School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Ballycastle High School
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

This policy applies to all members of Ballycastle High School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the ICT curriculum / PSHE curriculum. In addition, such topics may be covered as part of whole school assemblies, year assemblies and pastoral lessons. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know how to narrow down or refine a search;
  - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;
  - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
  - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and

related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

This school also:

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

- support is actively sought from other agencies as needed (e.g. the PSNI, EA) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. Incidents are reported to the school Designated Teacher for Child Protection or the member of Senior Management with responsibility for e-safety.
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the PSNI if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT Infrastructure

Email security

C2k recommend that all staff and pupils should be encouraged to use their C2k email system. It is strongly advised that staff should not use home email accounts for school business.

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Internet security

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal.

Where staff and pupils are using non C2k Equipment on the legacy network or if they are accessing the Internet through school provided non C2k connections, the school takes appropriate measures to safeguard this equipment against security breaches, as this equipment will not be protected by the C2k Education Network device security software. Access via this method will also not be subject to the same traceability and auditability that is afforded to the C2k managed equipment.

School website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers, VLE/ICT Co-ordinators and ICT Technician.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g.

info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;

- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning platform

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools LEARNING PLATFORM will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform;

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.
- The school's preferred system for social networking will be maintained and monitored by relevant staff in school.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the School or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school will use Video-Conferencing equipment and facilities under supervision and monitoring of the relevant class teacher.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the PSNI as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Equipment and Digital Content

- Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Students must follow the School's Mobile Phone Policy.
  All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Principal. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff are encouraged to refrain from planning to receive personal calls outside of break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. All users of Mobile Devices need to adhere to the school's BYOD Policy. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.