Ballincollig Community School, Innishmore, Ballincollig, Co. Cork.

Internet Safety: Acceptable Use Policy 2019

The aim of this **Acceptable Use Policy** is to ensure that students will benefit from learning opportunities offered by the school's Internet and IT resources in a safe and effective manner.

Internet use and access is considered a school resource and privilege.

Therefore, if the school Acceptable Use Policy (AUP) is not adhered to, this privilege will be withdrawn and appropriate sanctions-as outlined in the AUP –will be imposed.

It is envisaged that school and parent representatives will revise the AUP regularly.

This version of the AUP was created in February 2019.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Each student will be issued with a unique Computer Network Account username and password. This will grant them access to the school's ICT resources. Students must only use their own username at all times
- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will monitor regularly, students' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.

- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- The broadband service and associated Internet security is provided and managed by HEAnet. HEAnet actively manages all traffic to /from the Internet and filters traffic based on its internal content filtering rules.
- The internal network is a Microsoft Windows managed environment. Microsoft Windows servers control access to all devices via assigned user accounts and associated permissions.
- All students are provided with a username and password. This password is always controlled by the student. No other internal network user should have access to this password.
- The student username and password provides access to a personal storage folder on the school's server, where the student may store ongoing work. School systems backup this data at regular intervals.
- The desktop environment provided to students is restricted to only the services and applications deemed as required by the school.
- Printing services are made available to students under the control of the class teacher.

World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments and not acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's Acceptable Use Policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

- Students will use approved class email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, that contains a virus, is obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat are forbidden.

Social Media:

Students who use social network sites that contain:

- Postings that use the name of the school or a member of staff
- Postings that contain pictures or other images that identify staff or students in uniform
- Allow others to post such material

will face immediate suspension from school.

School Website /School Twitter Account

- Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.
- The website will be regularly checked to ensure that there is no content that compromises the safety of students/ pupils or staff.
- The publication of student work will be co-ordinated by a teacher.

- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission / content focusing on individual students will not be published on the school website without the parental permission. Photographs, audio and video clips will focus on group activities. Video clips may be password protected.
- Personal student information including home address and contact details will be omitted from school web pages.

Personal Media Devices:

All personal media devices, including mobile phones and wearables are to be turned off while within the school premises.

While Ballincollig Community School accepts that it is a student's right to have a mobile phone, this policy aims to maintain a safe, nurturing environment where the personal dignity and rights of all the members of the school community are preserved.

In order to assist the school in implementing this policy, parents/guardians are asked not to arrange to contact students by mobile phone at any time during the school day. Contact with the school may be made through the office at 021-4871740 and students are directed to use the office phone in emergencies.

- Where a student brings a mobile phone to school, the phone must be switched off and kept in a locker during the school day 9.00-3.45pm or 9.00-1.15pm on Wednesdays and may not be used for any purpose on school premises or grounds. No student may have a mobile phone on his/ her person.

- Students found in contravention of school policy will have phone/ personal media device confiscated for one day. The mobile phone /personal media device will be returned to parent /guardian at the end of the school day.

- No photographs can be taken or recordings, video or audio, made with mobile phones. Using phones in such a way can seriously infringe on people's rights and appropriate sanctions may be imposed.

- Incidents where students use mobile phones to bully other students or send offensive messages or calls will be investigated under the schools Anti-Bullying policy. It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the school may consider it appropriate to involve the Gardaí in such incidents.

- The school accepts no responsibility for replacing lost, stolen or damaged mobile phones. The safety and security of mobile phones is wholly a matter for students / parents/guardians.

- It is strongly advised that students mark their mobile phones with their names and use passwords to ensure that unauthorised phone calls cannot be made on their phones.

- **Sanctions for breach of these rules include the initial confiscation of the device and potentially, suspension.**

NB The use of personal devices while on school tour will be governed by the School Tour Policy.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension from school or expulsion from school. The school reserves the right to report any inappropriate activities to the appropriate authorities including the Gardaí.

Monitoring /Evaluation / Review

This policy, as amended was approved by the Board on 5th march 2019

This policy will be reviewed and updated regularly/annually, taking into consideration implementation issues that may arise.

Review Date: September 2019.