



**Coláiste Chill Mhantáin**  
**Internet Acceptable Use Policy**

---

## **Rationale**

Internet use and access is considered a school resource and privilege. Therefore, if the School IAUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the IAUP and the Code of Behaviour will be imposed.

This document should be read in conjunction with the School Anti-Bullying Policy, in particular, in the event of Cyber Bullying.

## **Goal**

The Internet and the World Wide Web (www) are an integral part of society and are therefore part of our students' learning programme. The aim of this Internet Acceptable Use Policy is to ensure the students will benefit from learning opportunities offered by the school's internet resources in a safe and effective manner.

## **General Terms of Use**

**NOTE: All Internet use is monitored.**

Serious or repeated breaches of these rules will be dealt with under the school's Code of Behaviour.

- Under no circumstances are the following permitted:
  - Misrepresenting the school in any way when using the facilities.
  - Gaining or seeking to gain unauthorised access to resources (hacking).
  - Using the Internet facility for illegal or fraudulent activities.
  - Sending or requesting messages or documents that are inconsistent with the school's policies and guidelines.
  - Using the facilities in ways that are considered to be malicious or unethical.

- Accessing pornographic or otherwise unsuitable sites.
  
- E-mail should not be used for business transactions and should not incur costs to the school or County Wicklow VEC without authorisation.
  
- Students are not permitted to access games on the internet.
  
- Care must be taken to ensure that the facilities are not misused either by students or staff. E-mail is only as secure as your password. The delivery, confidentiality and privacy of E-mail cannot therefore be guaranteed.
  
- The use of the Internet must not interfere with the normal running of the school.
  
- Staff should be vigilant in regard to the use of the Internet by students. Any suspicious or improper use must be reported immediately to the I.T. staff or to the Principal or Deputy Principal.
  
- Excess use of the equipment by the students should be noted and, if persistent, the I.T. staff should be alerted.

### **School Strategy**

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

- Internet sessions will be supervised by a teacher.
- Filtering software and a firewall / or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.

- Each student will be assigned a specific computer to use whilst in the Computer Room as per the seating plan.
- Students may not use any other Computer without the permission of the supervising teacher.
- Uploading and downloading of non-approved software, data files, image files, audio and video files will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal memory sticks (USB), CD-ROMs or other digital storage media in School requires the supervising teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school or its staff members into disrepute.
- Students will observe good etiquette at all times and will not undertake any actions that may bring the school into disrepute.
- Any use of the school's computing resources or internet connection that could be considered bullying is in breach of this policy and in breach of the Anti-bullying Policy and will be dealt with accordingly.
- Students must not Log-on using the Usernames of other Students. Students must never reveal their password to any other person as they remain responsible for all activity on their profile at all times.

## **World Wide Web**

Students must not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

Students will report accidental accessing of inappropriate material to the supervising teacher. The teacher must then record the incident in the Computer Room Record Book.

Students will use the Internet for educational purposes only.

Students will be made aware that the copying of information into assignments and failing to acknowledge the source constitutes plagiarism and copyright infringement.

Students will be asked not to disclose or publicise personal information unless for educational purposes and when approved only under the supervision of the teacher.

Downloading and uploading materials or images not relevant to students' studies is in direct breach of the school's Internet Acceptable Use Policy.

Any usage, including distributing or receiving information, school related or personal, may be monitored for unusual activity, security and/or network management reasons.

## **E-mail**

Students will not send or receive any material that is illegal, obscene, and/or defamatory or that is intended to annoy or intimidate another person.

Students must use their school E-mail address. Students will use these school E-mail accounts in class under supervision by or with permission from a teacher. Students will note that sending and receiving E-mail attachments using the approved school E-mail account is subject to permission from their teacher.

Students will not reveal their own or other peoples personal details, such as addresses, telephone numbers or pictures unless for educational purposes and under the supervision of the teacher.

Students must never arrange a face-to-face meeting with someone they only know through E-mails or the Internet.

### **Internet Chat**

Students will only have access to chat rooms, discussion forums, messaging or other electronic communication forums for educational purposes and with the permission of the supervising teacher.

Social Networking Sites (SNS), including but not limited to Facebook, ASKFM, Twitter; Chat Rooms, including but not limited to MSN Messenger, Gmail Chat, Skype and any other similar sites are not to be accessed.

The use of proxy servers is strictly forbidden.

Face-to-face meetings with any third party organised via Internet Chat are forbidden.

### **School Website**

The website when online will be regularly checked to ensure that there is not content that compromises the safety of students or staff.

The publication of students' work will be coordinated by a designated teacher.

Student's 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 video and audio clips focusing on group activities. Content focusing on individual students will not be published on the school website without Parental/Guardian approval.

Personal student and staff information including home address, contact details and e-mail addresses will be omitted from school web pages.

The school website will avoid publishing the name of any student in a photograph.

The school will ensure that the image files are appropriately named – and will not use students' names in image file names or ALT tags if published on the web.

Students will continue to own the copyright on any of their work published on the school website.

## **Personal Devices**

Students using their own technology in School such as leaving a mobile turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or video and/or audio recording is in direct breach of the school's Internet Acceptable Use Policy and of the school's Mobile Phone Policy and will be dealt with accordingly.

## **Legislation**

There is no specific Legislation governing Internet safety at School level. This is complicated by the fact that the Internet functions in a global context whereas the law functions in a localised one. The following pieces of Legislation however have relevance to Internet safety:

- Data Protection (Amendment) Act, 2003.
- Child Trafficking and Pornography Act, 1998.
- Interception Act, 1993.
- Video Recordings Act, 1989.
- The Data Protection Act, 1988.
- Postal and Telecommunications Services Act, 1983.

## **Sanctions**

Misuse of the Internet will result in disciplinary action. In extreme cases, suspension or expulsion in accordance with the School's Code of Behaviour may be applied. The School also reserves the right to report any illegal activities to the appropriate authorities.

## **Roles and Responsibilities – Teachers**

Teachers will assign specific places in the Computer Rooms and, where necessary, approved school E-mail accounts to each student in each class.

Teachers will closely supervise students use of computers at all times.

Teachers will explain and revisit the IAUP **in September and in January** of each academic year.

Teachers will ensure that students' Internet use will be planned, task-orientated and educational within a regulated and managed environment.

## **Websites for More Information**

- [www.barnardos.ie](http://www.barnardos.ie)
- [www.beinggirl.ie](http://www.beinggirl.ie)
- [www.ncpc.org](http://www.ncpc.org) (National Crime Prevention Council)
- [www.reachout.com](http://www.reachout.com)
- [www.spunout.com](http://www.spunout.com)

- [www.yourmentalhealth.ie](http://www.yourmentalhealth.ie) (Health Services Executive)
- Some helpful key search words: bullying, cyber bullying, teenagers, adolescence, Microsoft, Facebook, Twitter ...