



Acceptable Internet Use Policy for Staff and Students

The following document contains the ‘Acceptable Internet Use Policy for staff and students in Catholic University School.’

The policy focuses on incorporating best practice in framing guidelines for acceptable internet use in the school.

This policy was ratified by the CUS Board of Management on Monday, 12 December 2011.

A full discussion of the draft policy should then take place at the beginning of the academic year 2011-2012 for further amendments before the final policy is submitted to the board of management for approval.

This document is divided into three parts:

- (i) Policy of Guidelines for Staff on the use of IT Systems/Equipment in Catholic University School. (Pages 2 - 3)
- (ii) Policy of Acceptable Internet Use Policy for staff and students in Catholic University School. (Pages 4 - 6)
- (iii) Recommendation of the Committee. (Page 7)

1. Policy of Guidelines for Staff on the use of I.T. Systems/Equipment in Catholic University School

These guidelines have been drawn up in order to protect both the school and its employees from any inadvertent misuse of the IT facilities in Catholic University School.

(1) General Principles

Use of school Internet/e-mail by Catholic University School employees is encouraged and permitted where such use is for official business or training purposes and supports the goals and objectives of the school.

The high standards of professional and personal behaviour expected at all times of staff in the school extend to the use of the Internet and IT systems.

(2) Unacceptable Uses

The following uses of the school computer system are considered unacceptable. (This list is illustrative and not exhaustive).

(a) Access:

Unauthorised access to the computer system is not allowed. Similarly unauthorised access to any other computer system through the school system or exceeding your authorised access is not allowed.

The computer system may never knowingly be used to access material that is profane or obscene or that advocates illegal acts, or that advocates violence or discrimination towards other people

I.T. hardware/software may not be used for personal gain for gambling or to engage in any illegal act. E-mails that are for personal gain or profit may not be solicited

Harvesting e-mail addresses is not permitted on the school system

(b) Resource limits:

Large files must not be downloaded unless absolutely necessary. If necessary, such files can be downloaded at a time when the system is not being heavily used.

Deliberate attempts may not be made to disrupt the computer system or destroy data by spreading computer viruses or by engaging in sustained high volume network traffic that substantially hinders others in their use of the network.

Chain letters or 'spamming' must never knowingly be engaged in.

(c) Netiquette:

Private information about another person should never knowingly be posted.

Harassment or persistently acting in a manner that distresses or annoys another person is not permitted.

Restrictions in the use of in appropriate language apply to public messages, private messages and material posted on web pages.

(d) Plagiarism and Copyright:

The rights of copyright owners must be respected. If a work indicates that parts or all of it may be appropriately used, the expressed requirements must be followed.

Where it is unclear whether or not the work can be used, the permission of the copyright owner must be sought.

(3) Liability

Entering financial details on websites (credit card, laser card details) is done so at the individual's own risk.

2. Draft policy of Acceptable Internet Use for staff and students in Catholic University School, 89 Lower Leeson Street, Dublin 2.

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

Internet use and access is considered a school resource and privilege. Therefore, if the school's acceptable use policy is not adhered to this privilege will be withdrawn and appropriate sanctions - as outlined in (g) under 'Guidelines' - will be imposed.

It is envisaged that school and parent representatives will revise the acceptable use policy annually.

Before signing, the acceptable use policy should be read carefully to indicate that the conditions of use are accepted and understood.

Guidelines for Acceptable Internet Use

Conditions of use of the school's internet facilities

(a) General

- The use of networked devices in class is a privilege and not a right.
- Internet sessions are always supervised by a teacher.
- In class, a teacher's wishes regarding the use of networked devices must be followed.
- Teachers may confiscate any device which is being used inappropriately in class.
- The school ensures that students' internet usage is regularly monitored.
- Students and teachers are provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software is not permitted.
- Virus protection software is used and updated on a regular basis.
- Use of personal CD-ROMs or USB key in school requires a teacher's permission.
- Students observe good "netiquette" (i.e. etiquette on the Internet) at all times and do not undertake any actions that may bring the school into disrepute.
- Students must not access other students' files.

(b) World Wide Web

Access to on-line resources enables students to explore thousands of libraries, databases and information boards that help to develop their researching skills. The school believes that the benefits from accessing information resources exceed the disadvantages of on-line access. Filtering software is used by the school in order to minimise the risk of exposure to inappropriate material.

- Students must not visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students must use the Internet for educational purposes only.
- Students are familiar with copyright issues relating to online learning.
- Students must never disclose or publicise personal information.
- Students are 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.

(c) Email

- Students must use approved class email accounts under supervision by or permission from a teacher.
- Students must not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Students must not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students should never make arrangements for an unsupervised meeting with another person online without the permission of a teacher/parent.
- Students should note that sending and receiving email attachments is subject to permission from their teacher.

(d) Internet Chat

- Students only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums are only used for educational purposes and are always supervised.
- Usernames must be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat are forbidden.
- Access to social networking sites like 'Facebook' and 'Twitter' is not permitted.

(e) School Website

- Digital photographs, audio or video clips of individual students are not published on the school website. Instead photographs, audio and video clips focus on group activities. Video clips may be password protected.
- Personal Student information including home address and contact details are omitted from school web pages.

(f) Legislation

- Students and parents should familiarise themselves with the following legislation which is available in the General Office:
 - Child Trafficking and Pornography Bill 1997
 - 1993 Interception Act
 - Video Recordings Act 1989
 - The Data Protection Act 1988

(g) Sanctions

- Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, the student's future in school will be considered. The school also reserves the right to report any illegal activities to the appropriate authorities. Please refer to the Code of Behaviour of the school.

(h) Support Structures

There are key support structures and organisations that deal with illegal material or harmful use of the Internet. Examples are,

www.safe.ie

www.ncte.ie

www.skool.ie

3. Recommendations of the Committee

1. Staff should meet to agree on practical procedures regarding the access and use of computer room. This is necessary to facilitate access to the internet for students researching project work or career information.

A list of procedures should be placed on the wall in the computer room.

2. Copies of the following documents are kept in the office:
 - Child Trafficking and Pornography Bill 1997
 - 1993 Interception Act
 - Video Recordings Act 1989
 - The Data Protection Act 1988
3. Students and teachers are given information in the area of Internet safety.
4. The possibility of students and parents signing a permission form (sample provided on next page) upholding acceptable use policy.