The Institute of Education
79-85 Lower Leeson Street, Dublin 2
Tel: +353-1-6613511 | Fax: +353-1-6619050
info@instituteofeducation.ie | www.instituteofeducation.ie

TECHNOLOGY USAGE POLICY

SEPT 2015

1.0 Computer Usage Policy (CUP)

1.1 Aims/Objectives

The purpose of this Computer Usage Policy (CUP) is to ensure that students will benefit from learning opportunities offered by The Institute of Education's computer systems & network, in a safe and effective manner. Internet use and access is considered a school resource and privilege, to assist in the support of teaching and learning, research and information handling skills. Students Computer Accounts **WILL** be suspended if any of the policies below are breached.

1.2 General

Computer and wireless network access is provided as an information and learning tool and is to be used for school and curriculum related purposes and should not be used for personal use. All existing school policies and regulations apply to a user's conduct with e-mail and the Internet, especially (but not exclusively) those that deal with unacceptable behaviour; privacy; misuse of school resources; sexual harassment; information and data security; and confidentiality.

The Institute has software & hardware systems that can monitor and record all e-mail and Internet usage, and record each chat, newsgroup or e-mail message. The Institute reserves the right to do this at any time.

No user should have any expectation of privacy as to his or her e-mail and/or Internet usage.

1.3 Student Responsibilities

These responsibilities include:

1. Treating all equipment and fittings with care and respect at all times.
2. Only logging in via their own account and password. These details must not be shared.
3. CDs and memory sticks or other digital storage media are not permitted without express consent from the IT Department.
4. No food or drink (including water) is permitted in the Computer Lab.
5. No additional software should be installed on school computers.
6. The rights of others must always be respected.
7. Appropriate words/language should be used at all times, e.g. when saving files and folders.
8. Logging off correctly is essential at the end of each session for each student.

9. Attempting to disable, defeat, or circumvent any school security facility will be subject to disciplinary action. The Institute has installed routers, firewalls, proxies, anti-virus software, and other security systems to assure the safety and security of the School's networks.
10. Informing the IT Department immediately of any suspected access violation, breach in the security system or virus is the responsibility of each student.

1.4 Monitoring

Barracuda (www.barracudanetworks.com) is in operation for monitoring internet usage in the school. The purpose of this hardware is to:

- Filter harmful websites
- Manage time spent online
- Block or filter chat
- Protect personal information
- Customise filtering for each user

The Institute reserves the right to inspect any and all files stored either electronically or otherwise in order to ensure compliance with school policies. The Institute will use independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We will block access from within our networks to all known sites.
No user may use the school e-mail and/or Internet facilities to deliberately disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

1.5 Access Violations

It is not permitted to seek or gain access to any documents, data or programs, which are not directly required by you for your studies. The software which we use is licensed. It is illegal to make copies of any software which is on the school's computer systems.

1.6 Personal Devices

Personal devices such as laptops, mobile phones, tablets etc. are prohibited unless approval for their use is granted by the IT Department.

Sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving, is in direct breach of the school's Acceptable Usage Policy.

2.0 Internet Safety: Acceptable Usage Policy (AUP)

2.1 World Wide Web

The Institute will employ a number of strategies in order to maximise leaning opportunities and reduce risks associated with the Internet. These strategies are as follows:

- Students will use the Internet for educational purposes only
- Uploading and downloading of non-approved software will not be permitted
- Students will not undertake any actions that may bring the school into disrepute
- Students will not visit Internet sites that contain obscene, illegal hateful or otherwise objectionable materials.
- Students will never disclose personal information
- Students will be familiar with copyright issues relating to online learning
- Access to Internet chat rooms and social networking websites is prohibited
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, will be monitored for unusual activity, security and/or network management reasons.
- Although many accidental or careless actions can be rectified, doing so costs time and money, and it is not always guaranteed that complete rectification will be possible.

2.2 E-mail

- Students will not send or receive any material that is illegal, obscene, and 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 e-mails or the Internet

E-mail should not be used for:

- Personal Gain or profit
- Representing one self as someone else
- Propagating chain messages
- Knowingly altering or destroying the integrity of any information
- The defamation of, or allegations about, any individual or organisation
- Copyright infringement

- Commenting on any pupil or staff member or making fun of or in any way attempting to bully their fellow pupils or staff members

E-mail brings many risks to the school so students must be aware that:

- Their message may go to persons other than the intended recipient. Thus, they should be able to stand over everything they write
- E-mail messages can carry computer viruses which can be dangerous to the school's computer operations
- Letters, files and other documents attached to e-mails may belong to others and there may be copyright implications in sending or receiving them without permission

2.3 Social Networking

The Institute of Education does not authorise use of its name on any social networking site. Students found misusing such sites in relation to The Institute of Education or any of its students or staff will be subject to disciplinary procedures.

The school considers that any student who maintains a presence on such online sites is responsible for the content associated with their presence on such sites. Any student who brings The Institute of Education into disrepute through activity on the Internet will be subject to disciplinary action, up to and including expulsion.

2.4 Advice for Parents

It is important to stress at the onset that, due to the nature of the technology and the uses and abuses to which it is put, it is not possible to guarantee the safety of all students using the Internet or other on-line services. However, with appropriate precautions, it should be possible to greatly minimise the risks involved. It is widely believed that the potential benefits for students and teachers of using this technology far outweigh any risks involved.

Any dangers inherent in Internet use can be compared to similar risks associated with other electronic media. Adequate supervision is vital, as it would be in the case of a student's television or video viewing. Controlling access to the sites and services used and ensuring that students act responsibly while on-line are important steps in the process. Students should be informed that their on-line activities will be monitored and that they are accountable for their behaviour.

2.5 Legislation

The school will comply with the following legislation relating to use of the Internet and recommend that teachers, students and parents should familiarise themselves with the legislation:

- Child Trafficking and Pornography Act 1998-2004 (or any amendments)
- Video Recordings Act 1989
- Data Protection Acts 1988 – 2003 (or any amendments)
- Interception Act 1993
- The Freedom of Information Acts 1997-2006

2.6 Sanctions

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

3.0 Statement of Compliance

"I have read the School's Computer Usage Policy (CUP) and Internet Acceptable Usage Policy (AUP). I fully understand the terms of these policies and agree to abide by them. I realise that the School's security software may record for management use the e-mail and Internet address of any site I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be recorded and stored in an archive file for management use. I know that any violation of this policy may lead to disciplinary action being taken."

I accept these Terms and Conditions:

Signed: _____

Date: _____

Print Name: _____