DIT Students' Union-
Computing and Information Services Acceptable Use Policy.

Introduction:

DIT Students' Union is committed to providing efficient computing and information service resources, including e-mail and internet access, for staff use to aid their working activities. This document constitutes DIT Students' Union's policy and procedures for the acceptable use of all aspects of electronic information and communication utilising the company's Information Technology infrastructure.

In general, acceptable use means *respecting the integrity of the information and IT assets of DIT Students' Union Ltd. against external, internal, accidental and deliberate threats and to minimise the risk of damage by preventing security incidents and reducing their potential impact.*

As a user of these services and facilities, you have access to valuable company resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

The purpose of this document is to make users aware of what the company deems to be acceptable and unacceptable usage of the facilities and to provide guidelines for good practice.

Terms & Conditions;

In addition to the following Policy there are other areas you should pay attention to:

You must respect the laws of Ireland and specifically, but not exclusively, be aware of your responsibilities under:

- Copyright Act (1963) and as amended
- Data Protection Act (1988)
- Prohibition of incitement to hatred Act (1989)
- Criminal Damage Act (1991)
- Freedom of Information Act (1997)
- Child Trafficking and Pornography Act (1998)

In addition, there are company policies in a variety of areas under which all users must operate. These include:

- Mutual Respect & Dignity Policy
- Social Media Policy

Procedure Set One;

Acceptable use of computer equipment, including Internet access:

As a staff member of DIT Students' Union you may be provided with access to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy, and of protection from abuse and intrusion by others sharing these resources. In turn, you are responsible for adhering to the following procedures that illustrate appropriate use of the company's technologies and resources.

Accountability and Security:

Each user is individually responsible for appropriate use of all resources assigned to them, including the computer, software and hardware. In addition you must ensure, in so far as practicable, that the computers in your office or under your control are not used for unauthorised purposes. You should make a reasonable effort to protect your passwords and to secure resources against unauthorised use or access.

Privacy and Personal Rights:

DIT Students' Union is committed to maintaining the privacy of its users and does not actively monitor computer usage. However users should be aware that records are kept of all usage and could be made available in specific circumstances. All users of the company's network and computing resources are expected to respect the privacy and personal rights of others.

Personal Use:

The primary use of the company's computer equipment and Internet is for company related work. Incidental personal use is permissible provided it does not consume more than a trivial amount of resources and does not interfere with staff productivity. However, such incidental use will not be deemed a waiver of DIT Students' Union's right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis. If management deems that a staff member is abusing this personal use procedure they may be subject to disciplinary action.

Viruses:

You must take reasonable care to ensure that you do not transmit viruses or other malicious computer code to other users. To prevent computer viruses being transmitted through our systems unauthorised downloading of software is forbidden. All software downloads must be approved and delivered by the Communications Coordinator.

Unacceptable and Illegal Use:

It is not acceptable to view, download, transmit or store any offensive, indecent images or material. You may not use the company's computer systems to publish or transmit anything that is libellous or defamatory or is damaging to another computer system. No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements, including but not limited to downloading and/or distribution of music, movies, or any other electronic media via the Internet.

Procedure Set Two;
Acceptable use of Electronic Mail:

Email enables DIT Students' Union Ltd. staff to communicate promptly and efficiently with colleagues internally within the organisation and also provide a prompt and efficient service to clients/customers/suppliers externally. While email brings many benefits to DIT Students' Union in terms of communications, it does also pose significant risks which need to be managed.

Accountability and Security:
Each user is responsible for the content and use of their own account. Passwords should not be shared with others. Care should be exercised when confidential information (e.g., sensitive casework details) are transmitted using e-mail. Whereas the company will do its utmost to ensure privacy, it is not possible to guarantee the confidentiality of e-mails. Users of the facilities should be aware of the possibilities that electronic communications might be intercepted, copied, forwarded, printed or stored by others.

Privacy and Personal Rights:
While every effort is made to insure the privacy of DIT Students' Union email users, this may not always be possible. In addition, since employees are granted use of email systems to conduct company business, there may be instances when the company, based on approval from authorised levels, reserves and retains the right to access and inspect stored information without the consent of the user. Staff should also be aware that electronic mail, to from or within the company, may be the subject of a request under the Freedom of Information Act, 1997.

Be Respectful:
Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to company discipline as well as legal action by those who are the recipient of these actions. E-mail is easily forwarded. Due to the instant nature of email messages written and sent in haste could give rise to legal liability on the companys part. Always consider the possible implications of what you are writing before sending a message.

Representing DIT Students' Union:
The official DIT Students' Union signature should be sent at the end of all email messages. Email accounts should not be used for private purposes. Users may not, under any circumstances, use "spoofing" techniques or other means to disguise/masquerade their identities in sending email. The sending of unofficial or unsolicited bulk email is prohibited. You should not deliberately misrepresent your views as those of the company or any other person or organisation. Such action will be regarded as a serious disciplinary matter.

Unacceptable and Illegal Use:
Email facilities should not be used for any illegal purpose. It is forbidden to send or forward e-mails containing offensive or disruptive content, which includes, but is not limited to, defamatory, harassing, offensive, racist, sectarian, sexist, obscene or threatening remarks. If you receive an e-mail of this nature, you should immediately inform the Communications Coordinator.

Procedure Set Three;
Information Security Management:

Increasing amounts data and information used by DIT Students' Union are stored on electronic media (hard drives, portable devices, flash drives etc.). Such information can be sensitive and valuable, e.g., personally identifiable information, financial data, student casework, research, and other information considered sensitive. The exposure of sensitive information to unauthorised individuals could cause irreparable harm to the organisation and our members. If you have access to or are responsible for such data, you must ensure that the integrity, accessibility, accuracy and confidentially of such data are maintained.

Accountability and Security:
Each user of electronic media is responsible for the safekeeping of sensitive information on that device. Personal computers and computer terminals must not be left logged on when unattended and should be protected by key locks, screensavers with passwords or other controls when unattended, and that portable equipment in their custody is not exposed to opportunistic theft. All staff are required to use authorised encryption software on all devices in their charge. Also, sensitive or classified information, when printed, should be cleared from printers immediately.

Privacy:
No information technology resources can absolutely guarantee the privacy or confidentiality of electronic documents. Staff should, however, take reasonable precautions to protect electronic documents containing private and confidential information.

Data Storage & Housekeeping:
Every staff member is responsible for ensuring that all electronic records and files are suitably stored and archived. The established guidelines for file naming should be adhered to at all times. All company protocols surrounding information back-up should be facilitated.

Portable Devices:
Users of portable devices need to be particularly vigilant and take appropriate steps to ensure the physical security of the device at all times, but particularly when traveling or working away from your office. To protect confidential information access to all portable devices must always be controlled by the use of proper usernames, passwords and authorised encryption software. Confidential or sensitive information should never be stored on portable storage devices such as USB keys. Users of portable devices should use our online services (Google Drive, Do, Salesforce etc.) in order to create, share and view documents on their device. Users should sign out of all active accounts when they have finished their session.

Report Incidents:
All staff, should report immediately any observed or suspected security incidents where a breach of the company's security policies has occurred, any security weaknesses in, or threats to, systems or services to the Deputy CEO and Communications Coordinator. If you mislay a portable device you ***must report the loss to the Gardaí within 24 hours*** (ensure you obtain a reference number) and contact the Deputy CEO and Communications Coordinator immediately.

Penalties & Agreement:

A failure to abide by this policy may result in being denied access to computer resources as well as other proceedings.

This policy on acceptable computer and information services use supersedes all previous policies on acceptable computer use and will be amended from time to time as required. Any user of DIT Students' Union computer resources is deemed to have made him/herself aware of this policy.

I have read the DIT Students' Union Computing and Information Services Acceptable Use Policy detailed above, I understand the procedures contained therein and agree to observe them.

Signed: _____

Dated: _____