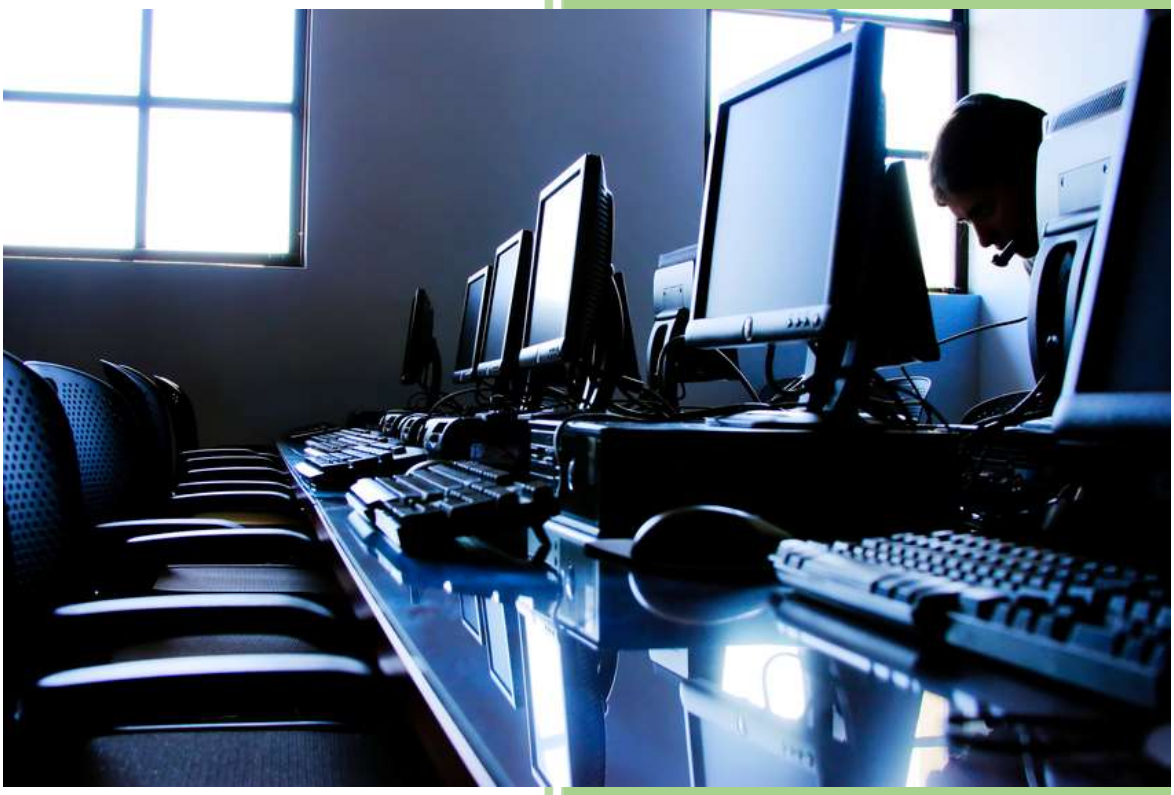
ICT Acceptable/Appropriate Usage Policy

Document Reference and Version No	ICT A/AUP / Version 2.2
Purpose	The purpose of this policy is to outline the acceptable and appropriate usage of IADT's ICT Resources.
Commencement Date	November 2020
Date of Next Review	October 2023
Who needs to know about this document	All Staff, Students and external parties using the Institute's ICT resources
Revision History	Minor Revision of 2.1
Policy Author	ICT Manager
Policy Owner	Directorate of Corporate Services
Approval by Governing Body	November 2020

ICT Acceptable/Appropriate Usage Policy



Information Services Division
Dun Laoghaire Institute of Art Design and Technology

Contents

1.0 Policy Overview

Dun Laoghaire Institute of Art, Design and Technology (IADT) is committed to educational, research and development activities across a wide range of sectors, from technology to humanities to the creative arts. We recognise the importance of stimulating creativity and innovation, and we also value the individual needs of staff and students in their daily lives. The Information and Communications (ICT) infrastructure of our organisation plays a vital role in maintaining and developing our profile, as well as the education environment in which we work.

IADT is publishing the ICT Acceptable / Appropriate Usage Policy (A/AUP) to facilitate its established culture of openness, trust and integrity and not to impose restrictions in relation to the use of current systems. The policy is to encourage responsible use of the network resources.

Whilst there is a need to keep our creative endeavours as free from constraints as possible, IADT is also required to ensure that there are some boundaries in place, so that individuals and the Institute are protected from the effects of what are illegal, inappropriate and anti-social uses of ICT.

IADT is committed to protecting its employees, students, partners and the Institute from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Purpose

The purpose of this policy is to provide a reliable computing and networking service. Access to communication devices for staff, students and alumni requires cooperation from all users. It is therefore important that you are aware of your responsibilities. The scope of this policy is to outline the acceptable and appropriate usage of IADT's ICT Resources.

By using any of Dun Laoghaire Institute of Art, Design and Technology (the "Institute")'s ICT Resources (as defined below), you agree to comply with the terms of this ICT Acceptable/Appropriate Usage Policy (the "A/AUP Policy"). This policy is without prejudice to the right to privacy as protected by the constitution and the European convention on human rights.

3.0 Scope

This policy applies to staff, students, alumni and/or external parties (as defined below) using the Institute's ICT Resources which includes, without limitation, its networks (regardless of how they are accessed) and/or communication devices. These systems are to be used for the purposes of serving the interests of the Institute, as a centre for teaching and learning in education.

The Institute networks and communication devices / systems as defined but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing, FTP, telecommunication systems (including IADT owned mobile phones) and IADT internet cloud presences (Office 365, Blackboard, AWS, Azure etc).

An EduRoam user visiting the Institute is in principle considered a visitor who wants wireless Internet access. The EduRoam visitor must abide by their home organisation's AUP or equivalent and the Institute's ICT A/AUP. Where regulations differ the more restrictive applies. Thus EduRoam visitors are considered as part of the ICT Users as defined below and need to be aware of this policy.

Institute ICT Resources include those provided centrally by the Institute's Information Services Division; those ICT Resources provided locally to its offices; departments; faculties; functional

areas and other units. It also encompasses Institute ICT Resources accessed remotely from any location without limitation:

(a) The Institute's network and connected networks and to all equipment connected to those network physically (directly or indirectly) or via wireless.
(b) Any network created independently of the campus network, whether they are connected to the Institute network or not.
(c) All Institute owned ICT equipment including but not limited to servers, desktops, laptops, tablet computers, personal digital assistants (PDA), mobile phones, other mobile devices, network related equipment and appliances.
(d) Any equipment owned by third parties, leased or personally owned which use the Institute's network, in conjunction with their work, research or study in the Institute.
(e) Any cloud services IADT has signed up too. Examples would include Blackboard, Office 365, Email, Online Forms, Virtual Desktops, Microsoft Azure resources, Amazon Web Services (AWS), Agresso, Core HR, Banner, Online Storage (OneDrive). Any future SAAS IADT may sign up too are also to be considered Institute ICT Resources.

For the purposes of this A/AUP Policy:

- Staff means all full-time and part-time employees of the Institute, including research staff funded externally and agency/contracted staff.
- Student means all full-time and part-time students of the Institute.
- Alumni means any former staff and students who retain permitted access to Institute ICT Resources.
- External Parties means all the Institute's subsidiary companies, contractors, consultants, researchers, visitors and/or any other parties including all personnel affiliated with third parties who have access to the Institute's ICT Resources.

Here after, collectively referred to as "Users".

This policy supersedes all prior policies on the subject and will be supplemented and/or amended as required and deemed necessary to address changing business and technical issues.

Use of the Institute ICT Resources constitutes a User's acknowledgement of and consent to the Institute's right to conduct monitoring and disclosure, as described above and agreement to comply with the provisions of this policy.

4.0 Policy

You must use the Institute's ICT Resources in a responsible manner and you must respect the integrity of computer systems, communication devices, networks and data to which you have access, and follow any standards and guidelines (including those set out in this Policy) relating to their use. By way of example, in order to comply with this ICT A/AUP Policy, you must make yourself familiar with the following.

4.1 General Use and Ownership

4.1.1 The Institute's ICT Resources are provided to support the activities of the Institute. Limited personal use of the Institute's ICT Resources is allowed, subject to the restrictions outlined below. Personal usage should never conflict with:

i. the primary business purpose for which the ICT Resources have been provided.
ii. the Institute's responsibilities, applicable laws and regulations.

Each User is personally responsible for ensuring that the terms of this Policy are followed.

4.1.2 Data on the Institute's systems (including documents, other electronic files, e-mail and recorded voicemail messages) is normally considered the property of the Institute within the scope of the Institute's research policies and except where this data is received from an external source in the course of academic business and therefore may be the property of the sender.

4.1.3 For security and network maintenance purposes, authorised individuals within IADT may monitor equipment, systems and network traffic at any time. Users are reminded that all files saved or accessed on Institute's computers and network servers are date, time and User ID stamped, as are all visits to websites outside the Institute. Mobile devices may also be monitored through the use of GPS data, "find my phone/device" type software service and other mechanisms to protect the device, the data stored on the device, the individual user of the device and the Institute.

4.1.4 Where the system allows encryption the IADT ICT Resource shall be encrypted.

4.1.5 The Institute's Information Services network administration endeavours to provide the highest level of privacy, the Institute does not provide Users with a guarantee of privacy or confidentiality in connection with the use of the Institute's ICT resources including email and internet systems. To protect its business, the interests of staff, students and others and to ensure compliance with this policy, Users should note that the Institute reserves the right to access, monitor, review and (where necessary disclose) Users' telephone log and calls, voicemail, e-mail (including personal/private e-mail or e-mail accounts accessed from or using the Institute's equipment), internet use and other common and communication facilities provided by the Institute which Users may use during their time with the Institute. This includes documents or messages marked "private", which may be inaccessible to most users. The deletion of a document or message may not prevent the Institute from subsequently accessing the item in question.

The Institute reserves the right to audit networks, systems and machines (including personal equipment connected to Institute ICT resources). An exception to this is the preservation of full confidentiality with regards to medical/health records held and associated computing systems.

The Institute will use this right reasonably, where necessary, in a targeted manner and for legitimate reasons but it is important that Users are aware that communication and activities on the Institute's ICT Resources cannot be presumed to be private. Some examples (not exhaustive) where monitoring may occur are set out below:

(i) Routine monitoring of e-mail traffic flow does occur. Such monitoring or examination may be made by Information Services technical personnel or supporting third party ICT contractors for system maintenance or operations purposes.

(ii) Electronic mail and voicemail messages are the property of the Institute. As with other Institute documents or records, the contents of any stored messages or files may be reviewed by management for legitimate business reasons which may include but not limited to:

a) reason to suspect that this A/AUP Policy is being breached,
b) ensure the provisions of this policy are being complied with particularly the protection of confidential information, the Institute's intellectual property, the defence of litigation and the detection of fraud,
c) for the investigation of any disciplinary offence (including any breach of this policy);
d) for the purposes of back-up and/or problem solving or where there are other legitimate reasons for doing so,
e) when the Institute is required to do so by law,
f) For Freedom of Information and/or Data Protection/GDPR requests,

g) where, without access to the information in the account, the operations or functions of the Institute or a Institute department, functional area or faculty are likely to be seriously obstructed or impeded or where there could be serious safety or financial implications,
h) where the account holder is no longer a member of staff or retired staff, management will be given access to Users e-mail, voice mail and other electronically stored information,
i) when an e-mail message is undeliverable (this is normally due to an incorrect address in which case the e-mail is redirected to the e-mail administrator who has to either open or redirect it accordingly or discard it).

(iii) The Institute may be required to disclose e-mail, voice mail and other electronically stored information to third parties pursuant to legal proceedings or governmental investigations or an access request made under Data Protection or Freedom of Information rules. The Institute may, where it receives a complaint from a third party, access and review e-mail, voice mail and other electronically stored information and where the Institute considers it is reasonable to do so. Although e-mails are commonly perceived to be instant and disposable in nature, they are often stored on a backup device. Further, recipients of messages may well have forwarded such messages onto third parties who Users may not know about. Generally, users should assume that all communications may be open to potential third party examination.

(iv) When a User leaves the Institute, management or other trusted staff member as assigned by senior management may be given access to his or her e-mail, voice mail and other electronically stored information.

4.1.6 Users should employ good house-keeping practices in the management of electronic documents such as employing a naming convention; having a backup schedule; deleting regularly; using passwords and producing paper copies if required to maintain the integrity of manual files. Electronic records should take on the same retention schedule as their paper counterparts see the Institute's Records Management schedule and Records Management Policy and GDPR records policy for guidance on how long a record (paper or electronic) should be kept.

4.1.7 Where there is a loss of data due to unlawful encryption (ransomware type attacks), corrupt data back-ups, ICT system failures or through hacking; IADT will not be liable for any loss of data held by an individual but not directly related to IADT on any of IADT's ICT Resources.

4.2 Security and Proprietary Information

Effective security is a team effort involving the participation and support of every User who deals with information and/or information systems.

4.2.1. It is the responsibility of every User to know or refer to the relevant guidelines as defined by IADT, Freedom of Information Act, the Data Protection Act and the General Data Protection Regulations (GDPR) confidentiality code and to conduct their activities accordingly.

4.2.2. Authorised users are responsible for the security of their passwords, accounts and any assigned equipment. Keep passwords secure and do not share accounts.

a) System level passwords should be changed yearly.
b) User accounts password should be changed every 90 days.
c) Password requires a minimum of 8 characters.

d) A User cannot use the last 15 passwords.
e) Failure to input the correct password more than 5 times results in the account to be locked for 30 minutes.
f) Users are encouraged to use a varied set of characters, including lowercase and uppercase letters, numerals, and symbols (like dots, colons, quote marks, dollar signs).
g) Some key and high security users can expect a greater level of protection through the deployment of multi-factor authentication (MFA) where the system allows. IADT will implement multi-factor authentication (MFA) where the system allows.

4.2.3. Personal data is very important, and it is equally very important to protect this data to the highest levels. All Users need to understand what personal data is and why it is so important that Users protect this data. Thus, for the purposes of the Institute the definitions contained in the Data Protection Acts, the General Data Protection Regulations (GDPR) and the Freedom of Information Acts are relevant to the Institute.

Personal data can be defined as: the individual's name, photograph, student number etc. Where any two or more pieces of such data are contained together, there is a higher risk of an individual being identified and therefore the Institute must take particular care that such information is properly managed.

Data Protection Acts 1988 to 2018 as amended

http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

"personal data" means data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller;

Regulation (EU) 2016/679 General Data Protection Regulations (GDPR) 2016

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Freedom of Information Acts 1997 to 2014 as amended

http://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/html

"personal information" means information about an identifiable individual that

a) would, in the ordinary course of events, be known only to the individual or members of the family, or friends, of the individual, or

b) is held by a public body on the understanding that it would be treated by it as confidential, and, without prejudice to the generality of the foregoing, includes

i. information relating to the educational, medical, psychiatric or psychological history of the individual,
ii. information relating to the financial affairs of the individual,
iii. information relating to the employment or employment history of the individual,

iv. information relating to the individual in a record failing within the definitions of the Freedom of Information Act 1997 to 2014 as amended,
v. information relating to the criminal history of the individual,
vi. information relating to the religion, age, sexual orientation or marital status of the individual,
vii. a number, letter, symbol, word, mark or other thing assigned to the individual by a public body for the purpose of identification or any mark or other thing used for that purpose.
viii. information relating to the entitlements of the individual under the Social Welfare Acts as a beneficiary (within the meaning of the Social Welfare (Consolidation) Act, 1993) or required for the purpose of establishing whether the individual, being a claimant (within the meaning aforesaid), is such a beneficiary,
ix. information required for the purpose of assessing the liability of the individual in respect of a tax or duty or other payment owed or payable to the State or to a local authority, a health board or other public body or for the purpose of collecting an amount due from the individual in respect of such a tax or duty or other payment,
x. the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name would, or would be likely to, establish that any personal information held by the public body concerned relates to the individual,
xi. information relating to property of the individual (including the nature of the individual's title to any property), and
xii. the views or opinions of another person about the individual,

4.2.4. Information can be contained on multiple devices. It is especially vulnerable on mobile type devices thus special care should be exercised when using such devices. It is recognised that authorised users of Institute data may need to carry personal data obtained by the Institute on portable storage mechanisms such as laptops or portable computers and/or portable storage devices such as memory sticks, mobile telephones, PDAs etc. This includes but is not limited to personal data regarding: staff members, students, research participants, campus visitors, invitees, telephone callers, event attendees and website visitors. In recognition of the security risks connected with the storage of such data on portable devices a number of good practices must be adhered to:

a) Authorised users should minimise the use of personal data on portable devices to that which is absolutely essential. Wherever possible only the specific data that is required should be transferred to portable devices.
b) Staff members should ensure that all normal security precautions are taken with Institute ICT Resources that are removed from Campus and with their own personal equipment, particularly where it holds personal data belonging to the Institute.
c) All Institute owned equipment will be password protected, encrypted (where possible) and these facilities must be used and not bypassed.
d) All personally owned equipment must be password protected to Institute standards and these facilities must be used. Where possible personally owned devices should also be encrypted.
e) All data files containing personal data of staff, students and or any third parties (examples but not limited to: research participants, event attendees, enquiry records, Institute records, Student Assessment details) must be encrypted.
f) All Institute files stored on portable equipment (which includes any files generated by the authorised user for use in any research or event connected in any way with the Institute) must be replicated in personal folders and/or functional area folders on Institute Servers. Such files must be regularly updated to be an exact replication of the portable file. This can be achieved where the staff member if off Campus for any prolonged period by e-mailing the file to their own Institute e-mail address.
g) All historical files containing personal data should be removed from portable devices when no longer required and such files should be regularly purged from such devices.

This is a requirement of the Institute's Records Management schedule, Records Management Policy and GDPR Policy.

h) Staff members are required to ensure that the browser's cache is deleted after every time Institute e-mail is checked on personal computers. This should be done by enabling the automatic deletion, where this is not possible or practicable the cache must be deleted after each session.

i) All files containing personal data being removed from Campus or outside the Institute network must be registered by e-mail with the Information Officer (Ms Angela Brennan 2018) as follows:

   i. Standard Notification
   This covers files of a standard nature regularly held on portable devices such as but not limited to class lists. This can be a regular (not less than annually) e-mail detailing the types of files (such as class lists) contained and the nature of the key primary data (such as the detail of the class and module).

   ii. Exceptional Notification
   This covers files not normally used by the staff member or where a regular notification has not been made.

   iii. The detail required for this register is as follows:
      - File Name;
      - Key Primary Data contained in the file;

   iv. Location of replica file on Institute ICT Resources;

   v. Purpose for which the file is being used off Campus;

   vi. All data must be secured through password protected files and folders where possible.

   Please note that the register will not be checked or verified by the Information Officer and the detail from the register will only be used where it is reported to the Institute that information and/or a portable device has been stolen, lost or mislaid and where the relevant staff member cannot be contacted.

j) All staff members are required to return all personal data owned by the Institute to their Manager and to purge such information from all personally owned portable devices, home computers and/or telephones and PDA's on leaving the employment of the Institute for whatever reason.

k) Any loss of equipment (Institute or personal equipment containing Institute Data) whether accidental (mislaid, damaged etc.) or enforced (confiscated or stolen) must be reported to the ICT Manager at the earliest possible opportunity.

4.2.5. Postings by staff or other members of the Institute from an IADT email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Institute, unless posting is in the course of Institute duties and where the originator has the necessary authority to act on behalf of the Institute in such matters.

4.2.6. All hosts used by the Users that are connected to the Institute Internet/Intranet/Extranet, whether owned by the Institute or not, must be continuously scanning for viruses and malware with a current virus/malware database. The operating systems should be patched to the latest releases, unless overridden by departmental or group policy.

4.2.7. Users of Institute email systems must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, ransomware or Trojan horse code.

4.2.8. The Institute encourages social media for academic and Institutional use. The Institute will offer guidelines to assist persons who wish to use social media for academic use and those who use official Institute social media sites. However all social media sites where used for

the purposes of academic or informational purposes on behalf of the Institute are bound by the ICT A/AUP.

4.2.9. The Institute and Users use of the Internet and mail services is bound by HEAnet's acceptable usage policies which is available at https://www.heanet.ie/about/our-policies.

4.3. Unacceptable Use

Under no circumstances is a User authorised to engage in any activity that is illegal under current legislation while utilising Institute ICT Resources or while connected to ICT Resources.

The items listed below are by no means exhaustive and attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations [including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Institute].

4.3.2 Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Institute or the end user does not have an active licence is strictly prohibited.

4.3.3 Software requiring a licence must not be installed until the licence is deposited with the ICT Manager.

4.3.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, ransomware etc.).

4.3.6 Revealing your account password to others or allowing use of your account by others.

4.3.7 Using an Institute ICT Resource to engage in procuring or transmitting material that the use, transmission or display of which may constitute bullying or harassment in violation of the Employment Equality Acts 1998 to 2004 or the Equal Status Acts 2000 to 2004 or the Institutes Mutual Respect Policy is strictly prohibited.

4.3.8 Users of an Institute ICT Resource actively procuring or transmitting any material that is in the Institute's sole discretion, unlawful, threatening, abusive, libellous, or encouraging of conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any current legislation. If in doubt about the acceptability of any material contact your Manager and/or the ICT Manager for guidance.

4.3.9 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties

4.3.10 Making fraudulent offers of products, items, or services originating from any Institute account

4.3.11 Port scanning or security scanning is expressly prohibited unless prior notification to the ICT Manager is made.

4.3.12 Executing any form of network monitoring which will intercept data not intended for the User's host, (unless this activity is a part of the employee's normal job/duty).

4.3.13 Circumventing user authentication or security of any host, network or account (unless this authority is part of the employee's normal job/duties).

4.3.14 Interfering with or denying service to any user other than the User's host (for example, denial of service attack or seizing operator privileges).

4.3.15 The provision of remote access to users is not permitted except through prior agreement with Information Services.

4.3.16 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.17 Providing information about or lists of Institute employees or students to parties outside the Institute, unless this activity is in discharge of Institute authorised duties and responsibilities.

4.3.18 Using internet relay chat (IRC) by a user on any Institute ICT Resource with the exception of those under direct control of Information Services. IRC includes robots such as bots and clones.

4.3.19 The Institute ICT Resources may be used to support charitable, professional organisational or community activities where approved in advance by Institute Executive management. The resources may not be used, however, to solicit for commercial ventures, religious or political causes, external organisations, or other non-job-related solicitations. Institute ICT Resources must not be used to advocate, further or otherwise support any business activities (other than those of the Institute) or illegal activities.

4.3.20 Users must make no attempt to gain access to the e-mail, voice mail or files of other Users. Users must not test, or attempt to compromise computer or communication system security measures. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered violations of the policy. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited. Exceptions to this policy may be made by management for the purpose of conducting tests of system security.

4.3.21 Sending "junk mail" or other advertising material to individuals who did not specifically request such material (email SPAM).

4.3.22 Unauthorised use, or forging, of email header information.

4.3.23 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.3.24 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.25 Use of unsolicited email originating from within the Institute's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Institute or connected via the Institute's network.

4.3.26 Internet access and e-mail should not, for example, be used for the following:
a) personal gain or profit,
b) to represent yourself as somebody else,
c) to advertise or otherwise support or engage in illegal activities,
d) to provide lists or information about the Institute or the Institute's staff or students to others and/or to send other confidential information without approval,
e) when it interferes with your responsibilities,
f) to promote political party policies or solicit political party membership.

This list is not exhaustive and will be added to where appropriate as additional network services are made available either locally in the Institute or through the Internet.

4.4 Email and Communications Activities

Each staff member within the Institute is provided with an email account to assist with their work for the Institute. Each registered student of the Institute is provided with an email account for their use. These email accounts are the primary way that the Institute will use to communicate with staff and students. Retiring staff may hold onto their email account for an agreed set period of time up to a maximum of one year and this must be agreed with their Manager and signed off by ICT Manager or SFC prior to retirement. Staff leaving the Institute for other reasons including career breaks may access their emails up to 30 days after they leave, this must be agreed with their Manager and signed off by ICT Manager or SFC prior to leaving. Non-staff members can have their email address ceased without any prior notice even where there was an agreement to grant short-term access. Email account holders must comply at all times with this ICT A/AUP Policy.

4.4.1 The email account of a staff member, and any information contained in it including content, headers, directories and email system logs, remains the property of the Institute. In general, the Institute will respect the privacy of a staff member's email account. However, the Institute does reserve the right to review, audit, intercept, access and disclose messages created, received or sent in certain circumstances as outlined in 4.1.4.

4.4.2 Any form of electronic bullying/harassment either by email, telephone, web comments/posts, messaging, through social media campaigns, or texting is not acceptable. Whether through language, visuals, content, attachments, frequency, or size of messages. The Institute's 'Mutual Respect' Policy will be called upon for guidance in handling this form of communication abuse.

4.4.3 Email traffic is monitored by Information Services to ensure efficient system performance and, when necessary, to locate problems/bottlenecks. Monitoring for this purpose may require an examination of the contents of messages.

4.4.4 Usage of the email system for academic and professional purposes is encouraged (articles, review papers, ebooks, review papers, professional bodies, etc.). Incidental use of an email account for personal purposes is allowed. However, systematic use on behalf of individuals or organisations that are not associated with the Institute or its business is not allowed. Personal use of e-mail is also subject to the same policies and regulations as official use.

4.4.5 All email messages may be subject to the Freedom of Information Acts (as amended, updated or replaced from time to time).

4.4.6 Great care should be taken when attaching documents to ensure the correct information is being released.

4.4.7 An email should be regarded as a written formal letter. Any defamatory or careless remarks can have very serious consequences. The use of indecent, obscene, sexist, racist or other

inappropriate remarks that may bring an individual or the Institute in to disrepute whether in written form, in cartoon form or otherwise, is strictly prohibited.

4.4.8 To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received.

4.4.9 Only send e-mail messages to those individuals for whom the e-mail message is relevant. The cumulative effect of unnecessary messages on e-mail systems can seriously degrade the performance of the system.

4.4.10 While messages should be accessed only by the intended recipient or delegates, the Institute cannot guarantee that only the recipient will read the message, staff should consider this when creating electronic messages. Staff members and students are not authorised to retrieve or read any e-mail messages that are not sent to them. Email messages must not be forwarded (redirected) automatically too external non-Institute accounts without prior approval from the Directorate of Corporate Services.

4.4.11 If you receive any offensive, unpleasant, harassing or intimidating messages via e-mail, Institute voicemail, Institute official social media sites or messages to your Institute mobile phone (where one has been assigned) you are requested to inform the Institute immediately emailing support@iadt.ie and your Manager.

5.0 Enforcement / Discipline

Any User found to have violated this policy may be subject to disciplinary action in line with the disciplinary procedures pertaining to each of the stakeholder groupings in the institute – these include the disciplinary procedures agreed with the TUI, FORSA (IMPACT), SIPTU, UNITE, the NUI and USI.

If any person is found to be in breach of The Copyright and Related Rights Act (2000) they shall in addition have such a breach addressed through the disciplinary procedures and may be held personally liable to the licencee/copyright owner for any damages that may arise.

Users must immediately advise the relevant members of staff of any suspected acts of violation, breach in the security system or virus so that such alleged acts may be investigated fully.

In the case of a data breach, loss of data or a breach of this policy the relevant Manager(s) will be informed as soon as possible and the Institute's Critical Incident Protocol will be implemented.

6.0 Further Information

If you have queries in relation to this policy, please contact:

ICT Manager

Dun Laoghaire Institute of Art Design and Technology

Tel: 012394777

Email: ict_manager@iadt.ie