lyit | Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Acceptable Usage Policy

September 2018

Contents

Revision History

Date of this revision: 12/09/2018		Date of next review: 12/09/2019	
Version Number/Revision Number	**Revision Date**	**Summary of Changes**	**Changes marked**
1.0	31/01/2014	Draft	
1.1	15/12/2015	Amendments proposed\accepted	
1.2	12/09/2018	Amendment to Appendix III on use by 3rd parties.	

Document Location

Website – Intranet	x
Website – Staff Hub	x
Website – Student Hub	x
Other:	

Consultation History

Version Number/Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
1.0	31/01/2014	HR	Draft forwarded to HR.
1.0	31/03/2015	Unions	Forwarded to unions via HR Office
1.1	1/1/2017	Unions	Agreement with Unions
1.2	12/9/2018	Unions	Change relating to 3rd parties access to LYIT email accounts Appendix III

Approval

This document requires the following approvals:

Name	**Title**	**Date**
HMG/ BB	Executive Board	10 September 2018
HMG	Governing Body	12 September 2018

This Policy was agreed by the Governing Body on 12 September 2018. It shall be reviewed and, as necessary, amended by the Institute on an annual basis. All amendments shall be recorded on the revision history section above.

1. PURPOSE

The purpose of this policy is to indicate the requirement for responsible and appropriate use of the Letterkenny Institute of Technology (LYIT) information technology (IT) resources.

LYIT provides resources to staff, students and external parties to assist them in performing their duties. It is envisaged that these resources will be used for educational, research and administrative purposes. This policy should be read in conjunction with LYIT's Code of Conduct and LYIT's Compliance policy. For details on LYIT's policy on the management of its social media presence please refers to LYIT's Social Media Management policy.

2. ROLES AND RESPONSIBILITIES

The following roles and responsibilities apply in relation to this Policy:

Governing Body	• To review and approve the policy on a periodic basis.
Registrar and Secretary/ Financial Controller	• To ensure the Policy is reviewed and approved by the Governing Body. • To consult as appropriate with other members of the Executive and Management Teams. • To liaise with Human Resources (HR) or Secretary / Financial Controller Office on information received in relation to potential breaches of the policy. • To ensure the appropriate standards and procedures are in place to support the policy.
IT Manager	• To define and implement standards and procedures which enforce the policy. • To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures. • To inform the Registrar or Secretary / Financial Controller of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.
HR Office and Secretary / Financial Controller	• To follow relevant and agreed disciplinary procedures when HR or Registrar's Office is informed of a potential breach of the policy (Refer to Section 7). • To manage the disciplinary process.
Staff/Students/External Parties:	• To adhere to policy statements in this document. • To report suspected breaches of policy to their Head of Department or the IT Manager.

If you have any queries on the contents of this policy, please contact the Registrar or the IT Manager.

3. SCOPE

This Acceptable Usage policy covers acceptable usage of:

- LYIT data
- LYIT resources

This policy applies but is not limited to the following, LYIT related groups as defined in Section 2.0 of the Overarching IT Documentation Framework:

- LYIT staff
- LYIT students
- LYIT external parties

4. SUPPORTING STANDARDS & PROCEDURES

- LYIT IT Documentation Framework;
- LYIT Information Security policy;
- LYIT Compliance policy (under development);
- LYIT Data Governance policy (under development);
- LYIT Social Media Management policy (under development);
- LYIT Password standard.
- LYIT Anti-Virus Scanning and Protection procedure;
- LYIT Encryption standard.

The above list is not exhaustive and other LYIT documents may also be relevant.

5. ACCEPTABLE USAGE POLICY

Conventional norms of behaviour apply to computer based information technology just as they would apply to more traditional media. Within the setting of LYIT this should also be taken to mean that the rights of academic freedom will always be respected. LYIT is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, social class, sexual orientation, age, disability or special need.

LYIT encourage all staff, students and external parties to apply a professional attitude towards their individual working environment, including the use of LYIT IT resources.

Staff, students and external parties are responsible for their individual user account and password details (Refer to LYIT Password Standard).

- No staff, student or external party shall jeopardise the integrity, performance or reliability of LYIT resources. Reasonable care 1must be taken to ensure that the use of resources does not reduce the level of integrity, performance or reliability of LYIT IT resources, or result in a denial of service to others.
- No staff, student or external party shall improperly/maliciously interfere or attempt to interfere in any way with information belonging to or material prepared by another end user.

[1] Staff, Students, and External Parties should reference LYIT's end user guidelines to ascertain what constitutes reasonable care.

- No staff member, student or external party shall make unauthorised copies of information belonging to LYIT, another staff member, student or external party. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.
- Do not redistribute or transmit information intended for internal use to parties who do not require it for Institute business use.

A limited amount of personal usage of LYIT resources is acceptable provided it:

- Does not consume more than a trivial amount of resources;
- Does not interfere with department or staff productivity;
- Is not for private commercial gain;
- Does not preclude others with genuine LYIT related needs from accessing the facilities;
- Does not involve inappropriate behaviour as outlined above, and;
- Does not involve any illegal or unethical activities.

In order to protect the interest of staff, students and LYIT, system based controls have been implemented to prevent inappropriate usage[2]. It is expressly forbidden under this policy to intentionally attempt to circumvent these controls.
While the above policy statements and principles apply to all types of IT resource usage including email, internet and social media, additional policy statements are provided in Appendices I, II and III to further clarify what constitutes appropriate usages of various LYIT IT resources.

6. MONITORING

LYIT respects the right to privacy of staff, student and external parties. However, this right must be balanced against LYIT's legitimate right to protect its interests and meeting legal obligations. LYIT is committed to ensuring robust information security and to protecting staff, students and external parties from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. To achieve its aims in this regard, LYIT reserves the right to monitoring of all LYIT information resources and LYIT data. Any monitoring of LYIT data and/or LYIT information resources is to ensure the secure, efficient and effective operations. The monitoring is non-intrusive and does not involve access or reading of content.

The Institute may at any time permit the inspection or disclosure of information held in LYIT's systems:

- When required by and consistent with the law. The Institute evaluates any such action against the precise provisions of the Freedom of Information Act 1997, Data Protection Act 2003, Copyright and Related Rights Act 2000, or other applicable law.
- At the written request of a duly authorised person in support of a bone-fide internal investigation instigated under another of the Institute's Policies.

All LYIT system activity including internet, email and social media activity is monitored electronically and logged for the following reasons:

- Monitoring system performance;
- Monitoring unauthorised access attempts;
- Monitoring the impact of system changes and checking for any unauthorised changes;
- Monitoring adherence to the acceptable usage rules outlined in this policy.

[2] Web Filtering solutions are one example of system based preventive controls.

When reviewing the results of any monitoring conducted in accordance with this section, LYIT will bear in mind that academic members of staff, students and external parties may be in possession of certain material for legitimate teaching, learning and/or research purposes. Academic members of staff, students and/or external parties will not be disadvantaged or subjected to less favourable treatment as a result of LYIT's monitoring provided they exercise their academic freedom within the law and can demonstrate that their teachings, research or qualifications are relevant to material detected and results revealed by Institute monitoring.

7. VIOLATION OF POLICY

Contravention of any of the above policy will lead to the removal of LYIT resource privileges and can lead to disciplinary action in accordance with the LYIT disciplinary procedures. Internet postings which are deemed to constitute a breach of this procedure may be required to be removed; failure to comply with such a request may in itself result in disciplinary action.

Note that; the Institute will fully co-operate with relevant authorities in investigating and prosecuting any illegal access or activity associated with the use of Institute resources or facilities.

Appendix I: General Acceptable Usage Guidance

- IT resources and internet facilities should only be used for legitimate LYIT purposes.
- IT resources and internet facilities should never be used in a way that breaches any of LYIT's policies.
- Users are provided with a dedicated single-sign on (SSO) account. The user is to use no other account on the network. The user should at all times keep the password of this account secure and private. The user takes full responsibility for the use or misuse of this account.
- The contents of all data repositories (mailboxes, disks, PCs, server shares, caches, etc.) operated in the Institute remain the property of the Institute.
- Data repositories are for Institute related storage only, for work, study, research and other approved activities; they are not to be used for personal data storage. Home and Public folders are sized for storage of documents only and are not intended for audio or video files.
- Any form of distribution mechanism or Intranet must be authorized by the IT Manager.
- With the exception of postgraduate students, all student home folders are wiped in June/July each year. Students should ensure that they have backed up their contents prior to this.
- Postgraduate student home folders will be wiped at the end of December each year, for students who have not re-registered on postgraduate programmes.
- Where a user brings their own PC, Laptop or tablet to the Institute for usage, the user retains full liability for the usage of this device and the legality of its content. Any connection is subject to conditions and such a device may not be connected to the Institute's wired network without prior written permission of the IT Manager or Senior Technical Officer; a wireless LAN has been provided for this purpose.

Appendix II – Acceptable Usage Rules for IT Resources and Internet Facilities

The following policy strictly forbids users to:

- Bring LYIT into disrepute.
- Breach any obligations relating to confidentiality.
- Defame or disparage LYIT or other staff, students, and/or external parties.
- Make inappropriate, hurtful or insensitive remarks about another individual or group.
- Harass or bully another individual or group in any way.
- Unlawfully discriminate against another individual or group. It is against the law to discriminate against another on grounds of gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of an ethnic minority.
- Represent yourself as another person.
- Obtain, store and/or transmit confidential LYIT information without appropriate authorisation.
- Breach data protection legislation (for example, never disclose personal information about another individual online unless this is done in compliance with the relevant legislation and LYIT authorisation).
- Breach any other laws or ethical standards.
- Ignore the legal protections to data and software provided by copyright and license agreements.
- Load unauthorised and/or unlicensed software onto LYIT Resources.
- Use LYIT IT resources to inappropriately obtain, store and/or distribute copyrighted material including music files and movies. Any such material found will be deleted without prior notification and the user account associated with the download suspended
- Use LYIT IT Resources to infringe intellectual property rights including trademark, patent, design and/or moral rights.
- Obtain/download, store and/or distribute text or images which contain any materials prohibited by law, or material of an inappropriate or offensive nature including pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity. Please note that access to certain pornographic sites may be a criminal offence (Child Trafficking and Pornography Act 1998). Any such suspected case will be reported to the Gardai.
- Use LYIT computers to make unauthorised entry into any other computer or network.
- Participate in unauthorised activity which results in heavy network traffic and thereby interrupts the legitimate use by others of LYIT resources.
- Disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse legislation3.
- Please note the following restrictions and other considerations:
- The Institute may filter access to certain Internet sites. User may have an expectation that sites with pornographic or adult material and sites involved in copyright infringement will be blocked.
- The Institute may block certain Internet sites from time to time for operational or security reasons; for example, some social networking sites have been blocked for access from Laboratory and library computers.
- Users are warned that under the Criminal Damage Act 1991, computer data is property and it is an offence to
- Add to, alter, corrupt, erase or move data to another storage medium or to a different location.
- Attempt to “hack” or gain unauthorised access to a computer, even if data is not damaged in the process”.

[3] Most computer crime related offences can be found in section 5 of the Criminal Damage Act, 1991 and Section 9 of the Criminal Justice (Theft and Fraud) Offences Act, 2001. The Council of Europe Convention on Cybercrime, which entered into force in July 2004, also provides guidelines for governments wishing to develop legislation against cybercrime.

Appendix III – Specific Acceptable Usage Rules for Email

- People should actively seek to use the most appropriate means of communication.
- E-mail may not be used for commercial purposes for personal gain except in the case of an approved contract entered into by the Institute including but not limited to; the catering provision, reprographics and banking services.
- Institute email communication can only be carried out on the Institute e-mail system, the use of 3rd party email systems to conduct Institute business is strictly forbidden.
- Users should not participate in the sending or distribution of chain messages, inappropriate or offensive messages, and advertising or in mass mailings of commercial or unsolicited information (SPAM).
- All views and opinions expressed in e-mail are the responsibility of the author. The Institute accepts no responsibility for such content. Users are warned that under the Electric Commerce Act (2000), e-mails are documents in writing rather than informal communications and may be considered as evidence of a contract and be legally binding
- E-mail servers are intended as communications mechanisms, not as storage repositories. Users should ensure that important information is not held on the mail server and that all critical mail and information is copied to a safe location (e.g. a home folder). Computer Services does NOT maintain backups of data held in the mail system.
- Storage limits are set on Institute mail servers. Where these limits are exceeded, mail services will be automatically suspended.
- E-Mail attachments from unknown or unsolicited sources should not be opened. These should be immediately deleted.
- Access to distribution groups such as “All Staff” and “All Students” lists is restricted to staff and to the students union and approved 3rd parties provided an approved contract is in place. “3rd parties can have access to email provided there is a contact or non-disclosure agreement in place confirming they will confirm to our email policy and compliance polices”. . Should any student want to post to these lists, they should forward the relevant message to the Student’s Union for consideration.
- The Institute reserves the right to automate the inclusion of disclaimers to Institute e-mails.
- Do not forward email messages where permission has been withheld by the originator.
- Do not (without prior notification to IT) forward electronic mail messages with attachments to large internal mail distribution lists.
- Do not remove any copyright, trademark or other proprietary rights notices contained in or on the email message.
- Do not use email to enter into legally binding contracts without proper authority being obtained beforehand.
- Do not use BCC to address recipients inappropriately.

Appendices IV – Specific Acceptable Usage rules for Social Media[4]

The policy statements in this appendix deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs, wiki's, and discussion boards.

The policy statements in this appendix applies to the use of social media whether during office hours or otherwise and regardless of whether the social media is accessed using LYIT's IT facilities and equipment or equipment belonging to members of staff or some other party.

The policy statements below are set out under three headings:

- Protecting LYIT's interests and reputation
- Respecting colleagues, students and others
- Protecting Intellectual Property and Confidential Information

Protecting LYIT's interests and reputation:

- LYIT staff should only use official Institute social media sites for communicating with students and external parties which are managed and moderated as outlined in Social Media Management policy. This includes the use of any social media presence related to the distribution of class materials, study aids, provision of feedback to students or any other supports for teaching and learning activities.
- Staff and external parties must not post disparaging or defamatory statements about:
- The Institute;
- Its Staff;
- Its Students; or
- Others.
- Staff, Students and external parties should also avoid social media communications that might be misconstrued in a way that could damage LYIT's interests and reputation, even indirectly.
- Staff, Students and external parties are personally responsible for what they communicate in social media.
- If your affiliation as a staff member, student or external party of LYIT is disclosed, it must be clearly stated that the views presented do not represent those of LYIT. For example, you could state, "the views in this posting do not represent the views of Letterkenny Institute of Technology".
- Avoid posting comments about sensitive work-related topics. Even if you make it clear that your views on such topics do not represent those of the Institute, your comments could still damage LYIT's reputation.
- Strive for accuracy in any material you post online.
- If you see content in social media that disparages or reflects poorly on LYIT or staff, students or external parties of LYIT, you should contact your line manager.

Respecting colleagues, students and others:

- Do not post material that could be deemed to be threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity.
- Do not post information including personal information related to LYIT staff, students and/or external parties without their express permission.
- Do not provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to LYIT and create legal liability for both the author of the reference and LYIT.

[4] Staff, Students and/or external parties should refer to LYIT's Policy for Social Media Management.

Respecting intellectual property and confidential information:

- Staff, Students and external parties should not jeopardise LYIT's business information, confidential information or intellectual property through the use of social media, internet file sharing or internet file storage sites.
- Staff, Students and external parties should avoid misappropriating or infringing the intellectual property of companies and/or individuals, which can create liability for LYIT, as well as the individual author.
- Staff, Students and external parties should not use LYIT logos, brand names, slogans or trademarks unless approved.
- Staff, Students and external parties should not post any of LYIT's confidential or proprietary information without prior written permission.
- Staff, Students and external parties should not post copyrighted material without citing appropriate reference sources or acknowledging copyright accurately.

Appendices V – Specific Acceptable Usage rules for Computer Laboratories

- A user must be in possession of a valid Institute ID card at all times. The user must present this card on demand to any Institute official. Failure to do so may result in a user being refused access to facilities.
- The user shall not in any way, tamper or misuse Institute equipment, either software or hardware. No form of tampering is acceptable. Activities such as installation of unauthorized software, changing screen saver, settings, etc. have an inherent cost to the Institute in terms of technician service time and will be treated as malicious tampering.
- The facilities are for Institute related educational and research use only. The facilities are not available for use on external projects or for work activities not associated directly with courses or the Institute. Facilities may not be used for any form of personal financial gain or commercial purposes.
- Computer laboratories are an expensive and finite resource. Users may not use computers for playing recreational games or for any other leisure or entertainment purpose.
- No food or drinks are allowed in computer laboratories. Smoking in computer laboratories and the Institute in general is similarly forbidden.
- The playing of music in laboratories, other than under supervision as part of a lecture, is strictly forbidden. Where student must play CDs or other music or audio files as part of their studies, headphones must be used.
- Users may not leave a computer to which they have logged on unattended. Users may not lock out computers for the use of others. Where computers found locked out or logged in but unattended, the user account will be disabled.

Appendices VI – Specific Acceptable Usage rules for Library Computer Suite

Access to Library Computer Resources imposes responsibilities and cooperation on part of the Computer User. The following Library Computer Use Policy, as well as the LYIT's Acceptable Usage Policy shall apply to all users of the Letterkenny Institute of Technology (LYIT) Library.

1. Internet Access: Library Internet access is for the sole purpose of (See also Appendix I):

    - Gathering and providing research material;
    - Preparing course material;
    - Completing class and homework assignments;
    - Searching catalogs and databases provided by LYIT library;
    - Search Internet for study, research and teaching.

2. Restrictions: Recreational and Social networking websites, such as Facebook, Bebo, YouTube, online gaming, etc. are prohibited. Currently 80% of computers in the Library Computer Suite will be filtering such content.
3. Responsibilities of Computer Users: LYIT requires Computer Users to respect the rights and sensibilities of all Library users. Some Internet sites are inappropriate for viewing in a public setting. Users should refrain from the use of sounds and visuals that may disrupt the ability of other Library patrons to use the Library and its resources. Library computers <u>are not</u> to be used for recreational purposes. Library and Computer services staff reserves the right to end computer use where there is inappropriate use of computer equipment.

Violations may result in the loss of Library Computer use and/or Library privileges.

Appendices VII – Specific Acceptable Usage rules for Wi-Fi Access

The Institute has established radio networks (Wi-Fi) for staff and student usage and for the use of visiting students and researchers.

- Student Wi-Fi LAN is intended for institute related usage only, by any user with a valid logon account. The service is generally available at all locations across Letterkenny and Killybegs campuses.
- Wireless networks are inherently insecure. Users should consider that any information transmitted across the wireless network is insecure. No Institute data (as per the data protection act) should be passed across Wi-Fi LAN.
- Users are instructed to treat the Wi-Fi LAN as a hostile environment. Users should have either personal firewall software or use the firewall software within their operating system.
- Users should ensure their PCs are updated with the latest operating system patches.
- Users should ensure their PCs have high quality anti-virus software, updated each day from the manufacturer's web site.
- In the event of a user's laptop showing any symptoms of virus infection, sequestering or disruptive configuration, and this laptop will be barred from access to the Wi-Fi LAN until such time as the user can demonstrate the issue has been resolved.
- Users requiring assistance to make a connection should call to the Institute's help desks. Although staff will give users advice and instruction on how to connect laptops to the Institute network, the responsibility for making this connection is solely the users. Users will be asked at this time to demonstrate that their equipment has been updated and patched and has a recent anti-virus release. LYIT staff will not directly carry out any configuration or remedial work on non-Institute equipment.
- All use of the Institute Wi-Fi LAN is entirely at the users own risk. No claims for damages will be entertained. The Institute is not responsible for student equipment or its damage when or if attached to any portion of the Institute network.
- Wi-Fi LAN has been tested with Windows 7, Windows 8 and Windows 10 and Apple OS X 10.x. Although other operating systems may work, staff may be unable to provide any technical advice for untested operating systems.
- The Institute currently supports IEEE 802.11a/b/g and uses CISCO access points based on CISCO LWAPP controllers.
- Any form of eavesdropping or monitoring of the wireless network and any form of unauthorized access is not permitted and will be subject to disciplinary procedures or criminal investigation.
- Access points may be authorized by the IT Manager only. Unauthorized access points will be considered a security breach and will be confiscated. The use of any devices in the 2.4 or 5 GHZ ISM band must be authorized by the IT manager. The use of Bluetooth devices is accepted.

Appendices VII – Specific Acceptable Usage rules for Software

Under no circumstances may software be installed on Institute equipment unless it has been authorised and correctly licensed.

1. All software in use in the Institute must be correctly licensed. On no account is unlicensed software to be used or copied to Institute computers.

2. The installation of software must be authorised by the IT Manager prior to its installation.

3. The Institute has a moral (and in some cases legal) responsibility to keep installation CDs and media secure. With this in mind.

4. Under no circumstances are media to be given, loaned or signed out to students, without the written permission of the IT manager.

5. Under no circumstances are media to be given, loaned or signed out to staff without the written permission of the IT manager. An exception exists when a standing order has been issued allowing release of CDs for practical classes or home usage (where licenses allow).

6. Software, which has been verified as licensed for use is detailed in the Computer Services Web Site. No other software is authorised to be loaded in laboratories or staff offices. No additional software is to be loaded on any Institute computer without written permission of the IT manager.

7. Where staff intend to use personally owned or purchased software on Institute computers, written permission should be sought from the IT Manager; documentary evidence of licenses should be included with this request.

8. The Institute takes no responsibility for software illegally installed on Institute equipment, in breach of this policy; the responsibility for such breaches lies solely with the individual involved.

lyit

Institiúid Teicneolaíochta
Leitir Ceanainn
Letterkenny Institute
of Technology

Bóthar an Chalaidh, Leitir Ceanainn
Contae Dhún na nGall, Éire

Port Road, Letterkenny
County Donegal, Ireland

Telephone + 353 74 918 6000
Fax + 353 74 918 6005

www.lyit.ie