
# Institute of Technology, Sligo

# Acceptable Usage Policy

# Version 0.2

## Document Location

The document is held on the Institute's Staff Portal here.

## Revision History

| Date of this revision: 28.03.16 | Date of next review: |
|---|---|

| Version Number/Revision Number | Revision Date | Summary of Changes | Changes marked |
|---|---|---|---|
| 0.1 | 25.11.14 | | |
| 0.2 | 28.03.16 | Replaced Head of Development and Business Operations with Secretary/Financial Controller or nominated member of the Executive Committee | |
| | | | |
| | | | |

## Consultation History

| Version Number/Revision Number | Consultation Date | Names of Parties in Consultation | Summary of Changes |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## Approval

This document requires the following approvals:

| Name | Title | Date |
|---|---|---|
| | Governing Body | 28.09.16 |
| | | |
| | | |
| | | |

This policy shall be reviewed and updated on an annual basis.

# Table of Contents

# 1. PURPOSE

The purpose of this policy is to indicate the requirement for responsible and appropriate use of IT Sligo's information technology (IT) resources.

IT Sligo 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 IT Sligo's Code of Conduct and IT Sligo's Compliance policy. For details on the IT Sligo policy on the management of its social media presence, please refer to the IT Sligo's Social Media 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.

**Secretary/Financial Controller or nominated member of the Executive:**

- To ensure the Policy is reviewed and approved by the Governing Body.
- To consult as appropriate with other members of the Executive and Senior Management Teams.
- To liaise with Registrar's Office or Human Resources (HR) 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 Secretary/Financial Controller or nominated member of the Executive of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.

**HR Office and Registrar Office:**

- 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 /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 Secretary/Financial Controller or the IT Manager.

## 3. SCOPE

This Acceptable Usage policy covers acceptable usage of:

- IT Sligo data;
- IT Sligo resources.

This policy applies but is not limited to the following:

- IT Sligo staff;
- IT Sligo students;
- IT Sligo external parties.

## 4. SUPPORTING STANDARDS & PROCEDURES

- IT Sligo Information Security Policy;
- IT Sligo Compliance Policy;
- IT Sligo Social Media Policy;
- IT Sligo Password Standard.

The above list is not exhaustive and other IT Sligo 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 IT Sligo, this should also be taken to mean that the traditions of academic freedom will always be respected. IT Sligo 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.

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

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

- No staff, student or external party shall jeopardise the integrity, performance or reliability of IT Sligo's resources. Reasonable care [1]must be taken to ensure that the use of IT resources does not reduce the level of integrity, performance or reliability of IT Sligo's IT resources, or result in a denial of service to others.

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

- 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.
- Similarly, no staff member, student or external party, shall make unauthorised copies of information belonging to 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.

A limited amount of personal usage of IT Sligo 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 IT Sligo 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 IT Sligo, 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 IT Sligo IT resources.

## 6. MONITORING

IT Sligo respects the right to privacy of staff, student and external parties. However, this right must be balanced against the Institute's legitimate right to protect its interests. IT Sligo 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, IT Sligo reserves the right to monitor all IT Sligo information resources and IT Sligo data. Any monitoring of IT Sligo data and/or IT Sligo information resources may be random or selective depending on circumstances at that time.

All IT Sligo system activity, including internet, email and social media activity, is monitored 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.

When reviewing the results of any monitoring, conducted in accordance with this section, IT Sligo will bear in mind that academic members of staff, students and external parties may be in

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

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 the IT Sligo'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 IT Sligo's monitoring.

## 7. VIOLATION OF POLICY

Contravention of any of the above policy will lead to the removal of IT Sligo resource privileges and can lead to disciplinary action in accordance with IT Sligo's 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.

# 8. APPENDICES

## Appendix I – Acceptable Usage Rules for IT Resources and Internet Facilities

IT resources and internet facilities should only be used for legitimate IT Sligo purposes.

IT resources and internet facilities should never be used in a way that breaches any of IT Sligo's policies.

In this context, the following policy statements apply:

- Do not bring the IT Sligo into disrepute.
- Do not breach any obligations relating to confidentiality.
- Do not defame or disparage IT Sligo or other staff, students, and/or external parties.
- Do not make inappropriate, hurtful or insensitive remarks about another individual or group.
- Do not harass or bully another individual or group in any way.
- Do not 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.
- Do not represent yourself as another person.
- Do not use IT resources to obtain, store and/or transmit confidential IT Sligo information without appropriate authorisation.
- Do not 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 IT Sligo's authorisation).
- Do not breach any other laws or ethical standards.
- Respect the legal protections to data and software provided by copyright and license agreements.
- Do not load unauthorised and/or unlicensed software onto IT Sligo resources.
- Do not use IT Sligo's IT resources to inappropriately obtain, store and/or distribute copyrighted material including music files and movies.
- Do not use IT Sligo's IT Resources to infringe intellectual property rights including trademark, patent, design and/or moral rights.
- Do not 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.
- Do not use IT Sligo computers to make unauthorised entry into any other computer or network.
- Do not participate in unauthorised activity which results in heavy network traffic and thereby interrupts the legitimate use by others of IT Sligo resources.

- Do not 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 legislation[3].

## Appendix II – Specific Acceptable Usage rules for Email

- People should actively seek to use the most appropriate means of communication.
- People should actively seek to use email distribution groups or lists in an appropriate manner.
- Do not forward inappropriate electronic mail messages to others.
- Do not forward email messages where permission has been withheld by the originator.
- Do not (without prior notification to IT Services) 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 CC or BCC to address recipients inappropriately.
- Do not use IT Sligo resources to participant in unsolicited advertising ("spamming").

## Appendices III – 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 IT Sligo's IT facilities or equipment belonging to members of staff or some other party.

The policy statements below are set out under three headings:

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

[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.

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

**Protecting the Institute of Technology Sligo's interests and reputation:**

- IT Sligo staff should only use official Institute social media sites for communicating with students and external parties which are managed and moderated as outlined in the Institute's Social Media 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;
    - It's staff;
    - It's students; or
    - Others.
- Staff and external parties should also avoid social media communications that might be misconstrued in a way that could damage IT Sligo's interests and reputation, even indirectly.
- Staff 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 IT Sligo is disclosed, it must be clearly stated that the views presented do not represent those of IT Sligo. For example, you could state, *"the views in this posting do not represent the views of the Institute of Technology, Sligo".*
- 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 IT Sligo's reputation.
- Strive for accuracy in any material you post online.
- If you see content in social media that disparages or reflects poorly on IT Sligo or the staff, students or external parties of the institute, 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 IT Sligo's 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 IT Sligo and create legal liability for both the author of the reference and the institute.

**Respecting intellectual property and confidential information:**

- Staff and external parties should not jeopardise IT Sligo's business information, confidential information or intellectual property through the use of social media, internet file sharing or internet file storage sites.
- Staff and external parties should avoid misappropriating or infringing the intellectual property of companies and/or individuals, which can create liability for IT Sligo as well as the individual author.

- Staff and external parties should not use IT Sligo's logos, brand names, slogans or trademarks without prior written permission
- Staff and external parties should not post any of IT Sligo's confidential or proprietary information without prior written permission.
- Staff and external parties should not post copyrighted material without citing appropriate reference sources or acknowledging copyright accurately.