Cork Institute of Technology

Acceptable Usage Policy

Version 2.0

Document Location

Currently located in IT Documentation folder of IT services site located on CIT Gateway

Revision History

Date of this revision: June 2016	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes	Changes marked
0.1	28/03/2013	Added in CIT references where required	
0.2	29/04/2013	Updates after union consultation meeting	
0.3	10/03/2015	Update with Acceptable Usage of Social Media	
0.4	01/03/2016	Updated with IT Department changes	
0.5	02/06/2016	Updated with feedback from consultation meeting	
2.0	17/06/2016	Updated with feedback from Audit Committee. Moved to version 2.0, version 1.0 was original policy written before IT Documentation Framework.	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
0.2	26/04/2013		- Clarified rights under disclosure policy - Referenced content scanning procedure - Removed violations sentence related to internet postings - Added clarity to scope of policy
0.5	31/05/2016		- Clarified definition of 'confidential' classification (section 10, App.1) - Clarified definition of ethical standards (section 10, App.1) - Clarified policy position in relation to licensed/unlicensed software (section 10, App.1) - Defined media owner (section 10, App.1) - Clarified how to dispose of media (section 10, App.1) - Clarified how to contact IT Services (section 10, App.2) - Reworded appropriate use of BCC (section 10, App.2) - Reworded registration with websites and added in further advice (section 10, App.2)

			- Highlighted guideline footnote in red (section 10, App.2)

Approval

This document requires the following approvals:

Name	Title	Date
Jonathan McCarthy	IT Manager	17/06/2016
Paul Gallagher	VP for Finance and Administration	17/06/2016

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 the Cork Institute of Technology (CIT) Information Communications Technology (ICT) resources.

This policy document covers all sections of Cork Institute of Technology (CIT).

CIT provides resources to all parties[1] 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 CIT Code of Conduct and CIT Compliance policy. For details on CIT policy on the management of its social media presence please refers to CIT Social Media Management policy.

2. DEFINITIONS

CIT Electronic Data
This refers to any electronic information stored, processed or transmitted using CIT resources.

CIT Resources
CIT Resources are any resources owned, licensed or provided for use by CIT. This includes but is not limited to the following:

i. Networks – wired and wireless (regardless of whether they are accessed remotely)
ii. PCs, Laptops, Macs, Servers
iii. CIT Mobile devices
iv. Storage - On-Premise and Cloud including but not limited to myCIT Google Drive, Office ProPlus Onedrive, CIT OneDrive for Business
v. Software systems and applications
vi. CIT USB memory devices

CIT Staff
All full-time and part-time employees of the Institute including research staff funded externally

CIT Students
All full-time and part-time under-graduate and post-graduate students of the Institute

CIT External Parties
All the Institute's subsidiary companies, contractors, researchers, visitors and/or any other parties who have access to CIT IT Resources

[1] "all parties" refers to students, staff and all external parties such as external contractors

3. 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 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 Registrar 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

All 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.

4. SCOPE

This Acceptable Usage policy covers acceptable usage of:

- CIT Data
- CIT Resources

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

- CIT Staff
- CIT Students
- CIT External Parties

By logging on to and/or using any CIT Resource whether directly or by remote access or by other means, all parties shall be deemed to have agreed to be bound by the terms of this Policy (as amended from time to time).

5. SUPPORTING STANDARDS & PROCEDURES

- CIT IT Documentation Framework
- CIT Information Security Policy
- CIT Compliance Policy
- CIT Data Governance Policy
- CIT Social Media Management Policy
- CIT Password Standard
- CIT Periodic Content Scanning Procedure
- CIT Disciplinary Procedure
- CIT End User Guidelines
- CIT Staff IT Administration Policy

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

6. 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 CIT this should also be taken to mean that the traditions of academic freedom will always be respected. CIT 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.

CIT encourage all parties to apply a professional attitude towards their individual working environment, including the use of CIT Resources. Furthermore, all equipment on loan from CIT to all parties must have a valid loan of equipment form approved by the relevant Head of Department.

All parties are responsible for their individual user account and password details (Refer to CIT Password Standard).

- No staff, student or external party shall jeopardise the integrity, performance or reliability of CIT resources. Reasonable care[2] must be taken to ensure that the use of resources does not reduce the level of integrity, performance or reliability of CIT ICT 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.
- Similarly no staff member, student or external party shall make unauthorised copies of information belonging to CIT, 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[3].

A limited amount of personal usage of CIT 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 CIT 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 CIT, system based controls may be implemented to prevent inappropriate usage[4]. It is expressly forbidden under this policy to intentionally attempt to circumvent these controls.

[2] Staff, Students, and External Parties should reference CIT end user guidelines to ascertain what constitutes reasonable care.

[3] This provision will not negate any rights inherent under the Disclosure (Whistle-Blowing) Policy

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

While the above policy statements and principles apply to all types of resource usage including email, internet and social media, additional policy statements and guidelines are provided in Appendices I (policy), II (policy) and III (guidelines) to further clarify what constitutes appropriate usages of various CIT resources.

7. MONITORING

CIT respects the right to privacy of all parties. However, this right must be balanced against CIT's legitimate right to protect its interests. CIT is committed to ensuring robust information security and to protecting all parties from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. To achieve its aims in this regard, CIT reserves the right to monitor all CIT Resources and CIT Data. Furthermore, CIT reserves the right to install estate management software to all IT devices owned and/or managed by the institute. Any monitoring of CIT data and/or CIT information resources may be random or selective depending on circumstances at that time and will only be conducted following direction from an authorised individual. The college may also monitor in circumstances where it is required to do so by law. Further information can be found in the **Periodic Content Scanning Procedure**.

All CIT system activity including internet, email and social media activity may be 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.

By using CIT Resources, all parties consent to all such monitoring, logging and scanning.

When reviewing the results of any monitoring conducted in accordance with this section, CIT will bear in mind that academic members of staff 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 CIT 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 CIT monitoring.

8. VIOLATION OF POLICY

Contravention of any of the above policy may lead to the removal of CIT resource privileges and can lead to disciplinary action in accordance with the CIT Disciplinary procedure.

If you want to report a suspected security breach of this Policy please contact your Head of Department or the IT Manager as may be required.

9. GENERAL

Headings used in this Policy and in the Appendices are for ease of reference only and shall not affect their construction.

Unless the context otherwise requires, any reference in this Policy to any gender includes the other and to the singular shall include the plural and vice versa.

Words not otherwise defined in this Policy that have a well-known and generally accepted technical or trade meaning in the IT industry in Ireland are used in this Policy in accordance with such recognised meaning.

Unless otherwise defined therein, capitalised terms used in Appendices shall have the same meaning as given to them in this Policy.

This Policy is reviewed periodically as required and CIT reserves the right to amend it at any time as it sees fit.

This Policy supersedes and replaces any previous policy relating to its subject matter. In the event of any inconsistency between the provisions of this Policy and the provisions of the content included in attached Appendices to this Policy, the provisions of the Policy shall take priority.

10. APPENDICES

Appendix I (Policy) – Acceptable Usage Rules for ICT Resources and Internet Facilities

CIT's ICT resources and internet facilities should only be used for legitimate CIT purposes.

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

In this context, the following policy statements apply:

- Do not bring CIT into disrepute
- Do not breach any obligations relating to confidentiality
- Do not defame or disparage CIT 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 obtain, store and/or transmit confidential[5] CIT 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 CIT authorisation)
- Do not breach any other laws or ethical[6] standards
- Respect the legal protections to data and software provided by copyright and license agreements
- Do not load any licensed software onto CIT Resources[7] unless you are sure CIT is in compliance from a license payment perspective
- Do not load any illegal[8] software onto CIT Resources
- Do not use CIT ICT resources to inappropriately obtain, store and/or distribute copyrighted material including, but not limited to, music files and movies
- Do not use CIT ICT resources to infringe intellectual property rights including, but not limited to, trademark, patent, design and/or moral rights
- Do not obtain/download, store and/or distribute text, images and videos 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 CIT computers to make unauthorised entry into any other computer or network

[5] Please see the Information Governance policy for a definition of what constitutes confidential information
[6] Please refer to the Ethics in Public Office Act 1995 for a definition of what constitutes ethical standards
[7] Please see section 2 for a definition of what constitutes a CIT resource
[8] For example, Bit Torrent software is one example of illegal software

- Do not participate in unauthorised activity which results in heavy network traffic and thereby interrupts the legitimate use by others of CIT resources
- Do not use CIT resources to participant in unsolicited Advertising ("spamming")
- Do not use CIT resources for social networking which significantly exceeds that required for CIT related work.
- Do not connect a non CIT device to the CIT wired network unless it has been pre-cleared[9] by a local IT technician to confirm it does not pose any risk to CIT
- 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[10]
- It is the responsibility of the media owner[11] to ensure that all media is disposed of properly and safely. Owners must ensure that no CIT data is left on devices that have been disposed[12].

[9] Non CIT devices must be pre-cleared by an IT technician in advance of every connection made to the CIT wired network

10 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.

[11] Owner is defined as the budget holder who approved the purchase requisition

[12] Please contact your local IT Technician for details on how to dispose of media appropriately

Appendix II (Policy) – Specific Acceptable Usage rules for Email

Staff are provided with an email account to assist with their work for CIT. Each registered student is provided with an email account for their use. This account is the primary way that the college will use to communicate with students. Email account holders must comply at all times with this AUP Policy.

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 college.

The college reserves the right to review, audit, intercept, access and disclose messages created, received or sent in certain circumstances:

- There is reason to suspect that this AUP Policy is being breached;
- For the purposes of back-up and/or problem solving or where there are other legitimate reasons for doing so;
- When the college is required to do so by law;
- Where, without access to the information in the account, the operations or functions of the college or a college department are likely to be seriously obstructed or impeded or where there could be serious safety or financial implications;
- Where the account holder is no longer a member of staff; and
- 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).

Email traffic is monitored by IT 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.
Incidental use of an e-mail account for personal purposes is allowed. However, systematic use on behalf of individuals or organisations that are not associated with the college or its business is not allowed. Personal use of e-mail is also subject to the same policies and regulations as official use. Care should be taken when attaching documents to ensure the correct information is being released.

All email messages may be subject to the Freedom of Information Act 2014 (as amended, updated or replaced from time to time).
Any defamatory or careless remarks can have very serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited. Staff members and students are not authorised to retrieve or read any e-mail messages that are not sent to them.

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 and must not be forwarded.

- If you receive any offensive, unpleasant, harassing or intimidating messages via e-mail, you are requested to inform IT Services immediately by phone at ext 5050
- People should actively seek to use the most appropriate means of communication
- 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
- Be mindful of your use of BCC to try and address recipients fairly and appropriately[13]
- Be mindful of a website's data usage policy when using your CIT email address to register with websites
    - The website may openly state that they will sell your details, thus exposing you and CIT to SPAM
    - Be mindful of how to unsubscribe from such registrations if you need to do so
- Do not use CIT resources to participate in unsolicited advertising ("spamming")
- Do not attempt to make CIT staff aware of email spamming or phishing attempts by forwarding the offending email to all CIT staff[14]
- The email address CIT@cit.ie is to be used for official CIT business communications only

[13] An example of appropriate use of BCC is when sending an email to many parties who need to be informed of something, while not wanting to expose every person's email address publicly

[14] If you need advice call the service desk by telephone. Please do not forward the offending email to anyone

Appendix III (Guidelines) – Guidelines for the Use of Social Media in the Academic Context[15]

Preamble and Definitional matters

One of the first problems to address in developing guidelines for the use of social media in any context is definitional. What do we mean by social media? What gets to count as social media?

The gamut is very broad. Social media clearly incorporates well-known social networking sites such as Facebook and microblogging sites such as Twitter but technically also incorporates important but wildly diverse sub-categories such as instant messaging, Voice Over IP (VoIP), virtual worlds and location-based apps and games and personal websites or blogs. In addition there are a number of walled or enclosed social media spaces and services such as the wiki and blogging tools inside the Blackboard LMS or certain social and sharing features within internally facing communication platforms such as MS SharePoint. All of this means not only that many subcategories of social media exist but that guidelines pertinent to one may not be appropriate or even make sense for another.

It is also the case that convergence and synthesis are ongoing. Existing social media subcategories, for example, are constantly growing into each other: online games now typically incorporate VoIP; Facebook offers location-based check-ins; and many social media apps allow for log in via Facebook or Google as standard. Moreover what we might refer to as "ordinary" web sites and services are becoming increasingly more "social", offering more and more prominence to the user reviews, content sharing, communication etc. This can make the distinction between social media subcategories hard to maintain and even raise questions about the inherent distinction between the social web and the "rest of the web". Again this creates a further level of complexity with regard to identifying where guidelines should be offered and/or followed.

Notwithstanding these difficulties the following definitions are offered by way of supporting some initial guidelines for the use of social media in the academic context.

- Digital identity: the persona an individual presents across some or all the online communities he or she is a member of (in some cases perhaps even unwittingly).
- Digital footprint: all the data created or "left behind" by a user's interactions in online spaces and though the use of networked gadgets, devices etc.
    - Can also refer to the size of one's "online presence", i.e. how many other users one relates to or interacts with.
- Social media: online social spaces and services with an emphasis on the creation and sharing of ideas, content, and media.
- Social networking service: a platform specifically to build and create social networks and virtual communities. Typically such services provide a profile for each user with their links to other users and a range of other communication and content sharing tools. Examples include Facebook and Google +. Social networking formally includes more than the use of social networking services and, by some definitions, includes any grouping together of individuals into specific social groups or any deliberate activities by their individuals to that end.

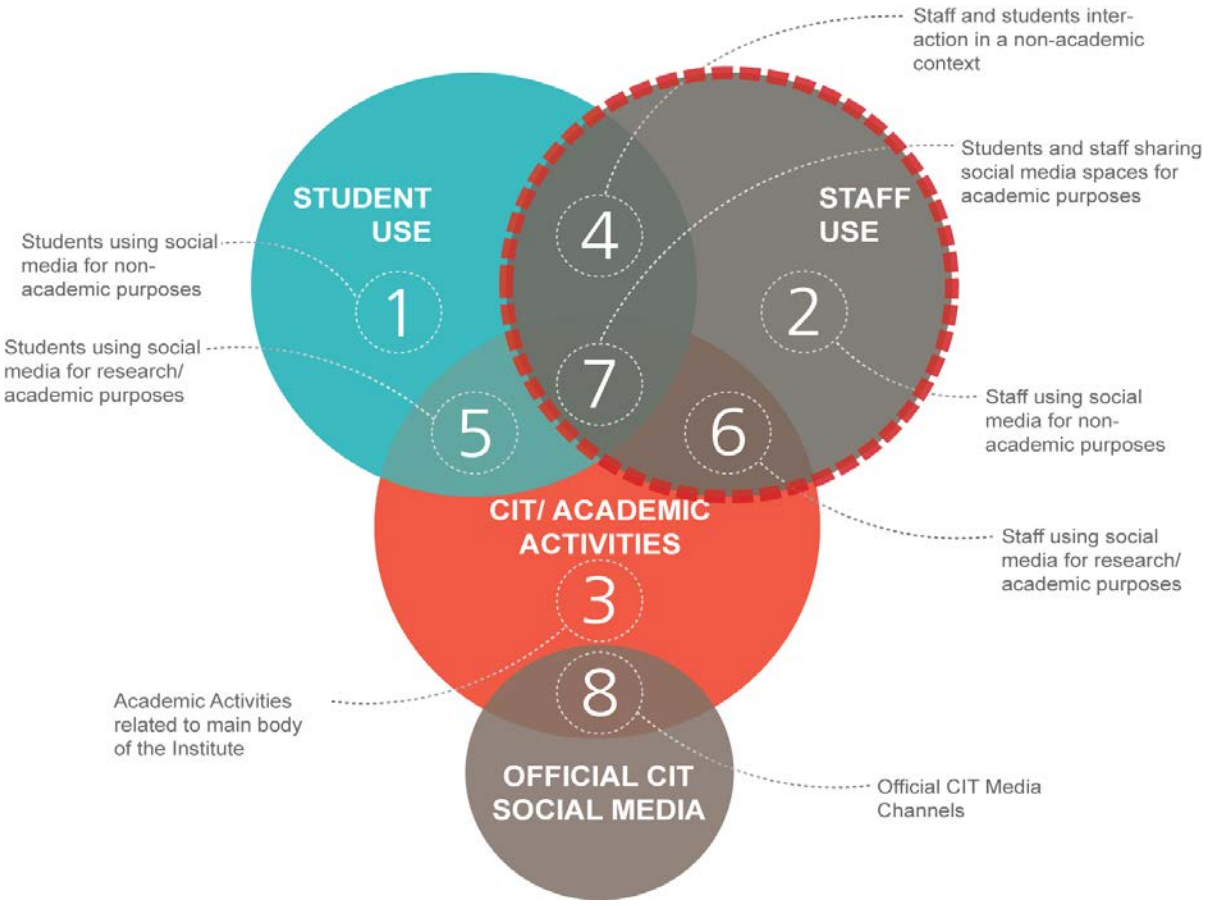
[15] Staff, Students and/or external parties should refer to CIT Policy for Social Media Management.

Introduction: Purpose and Scope

Establishing guidelines for the use of social media is complex for reasons outlined in the preamble but there is added complexity or need for care in the academic context as any guidelines here must also be sure not to infringe on academic freedom and not to stifle or discourage legitimate academic innovation.

With this in mind, an effort is made, first, to make clear where any guidelines at all can be offered. Secondly where any guidelines are offered these, as far as possible, have been limited to precepts and principles rather than, e.g., rules or dictates. Such precepts and principles, finally, are offered only to address online activities and practices with clear legal, ethical and/or reputational implications for the institute and its staff.

In making clear the scope or jurisdiction of these guidelines and in determining under what circumstances, by design or otherwise, staff and students might begin to occupy and interact in the same social media spaces, the diagram below is offered. In basic terms it offers a visualisation of student and staff use of social media as domains that can be separate or intersecting and which may, further insect in an academic or non-academic context. This diagram is used a way to suggest in the section that following different guidelines or advice that might apply to cover different kinds of use of social media with differeing kinds of, e.g. legal or ethical implications. As indicated later, however, social media has the unique ability to cross or collapse professional/personal and other traditional social boundaries so many of the visual distinctions made in the diagram, while – hopefully – conceptually useful, may be harder to maintain in reality.



Guidelines and Precepts

In this section the uses of social media by staff and students described above and the various ways, more importantly, in which staff and students might begin to occupy and interact in the same social media spaces are used to suggest some guidelines for practice. Certain guidelines apply to more than one area, e.g., guidelines for staff using social media for non-academic purposes are repeated again in the guidelines for staff and student interaction in non-academic contexts. Some guidelines are unique to one single area of activity, e.g. some very brief but specific advice is given with regard to intellectual property and confidentiality in context of staff use of social media for academic or research purposes, advice which does not appear elsewhere in the document. Some of the numbered areas from the diagram above do not attract guidelines at all either because they are already subject to some other guidelines or procedure and/or because – as in the case of CIT/Academic Activities – the area is simply being used to indicate a particular domain of practice so its interaction with other online activities can be accommodated into the diagram.

Throughout, again, the intention is to suggest things for staff to be cognisant rather than hard rules or regulations that need to be adhered to.

1. Students using Social Media for Non-Academic Purposes

Students typically use social media for non-academic purposes, for online socialising, to express personal views, to share content. Such use leaves a *digital footprint* however that may be carried across to certain other areas, e.g. 4, 5, and 7 in the diagram above. Such use can also permeate to the wider CIT community and to the general public. No guidelines for the student use of social media are offered here though other guidelines and/or policy documents may apply.

2. Staff using Social Media for Non-Academic Purposes

Staff additionally use social media for non-academic purposes, for much the same purposes as students: for online socialising, sharing content and views etc. Such use also leaves a digital footprint that may be carried across to certain other areas, e.g. 4, 6, and 7. Such use can again permeate to the wider CIT community and to the general public in ways that may impact, positively or negatively, on the reputation of the institute and which may also have ethical and legal implications.

In this context it is suggested that:

- All academic staff making use of social media should try to be cognisant of the persistence, replicability and visibility of any comments or content they add on social media sites and, as appropriate, take care not to share any confidential or proprietary information.
- Where one's identity as an employee of the institute has been made explicit, that one's own personal views, where possible, should be distinguished from those of the institute.

3. CIT/Academic Activities

There are a vast number of activities which "count" as being academic or as relating to the main business of the institute. Some of these can be conducted in online spaces or supported by same. This circle is just used to indicate this domain and where it might intersect with other online activities. A number of policies are already in operation here.

4. *Staff and Student Interaction in Non-Academic Contexts*

Staff and students, by design or by coincidence, can encounter each other and share the same social media spaces in a non-academic context. They might follow each other on Twitter, friend each other on Facebook or connect on LinkedIn. This can also be a legitimate and natural basis for use of social media by staff and students for academic purposes [7] but may also be preceded by [7], e.g. a lecturer might first invite students to use Facebook for academic purposes, in this case they then also end up sharing the same social media spaces in a non-academic domain. Either way various issues can arise in the context of the notion of a digital footprint or digital identity which are carried over from [1] and [2].

Once again the following principles are offered from 2 above:

- All academic staff making use of social media should try to be cognisant of the persistence, replicability and visibility of any comments or content they add on social media sites and, as appropriate, take care not to share any confidential or proprietary information.
- Where one's identity as an employee of the institute has been made explicit, that one's own personal views, where possible, should be distinguished from those of the institute.

In addition:

- The rights of students to maintain a separation between their identity as students and their identity in other private and public spheres should be respected where possible, along with their usual rights and freedoms as students.
- That staff should take care to ensure that their online relationships with students in the non-academic context cannot be seen to impact in significant ways, either positively or negatively, their relationship with students in the academic context. This applies particularly with regard to any perceiving influencing of the marking and feedback of student work or the provision of resources or facilities to students.

5. *Use of social media by students for academic or research purposes*

Students may quite naturally make use of social media for academic or research purposes or in ways that relate to academic or research activities. Such practices may, for instance, include tweeting about academic work, or student project groups using a Facebook page for project management.

Although such practices, and the online spaces and artefacts to which they give rise, could recognisably be linked to the institute it is not within the remit of this document to offer any guidelines in this area.

6. *Use of social media by staff for academic or research purposes*

Use of social media by staff for academic or research purposes, e.g. using Twitter to share and gain insights into a research topic; developing a work-related persona via LinkedIn or Academia.edu; conducting research using social media tools; using social media for administrative or productivity purposes. Such use often permeates to the wider community and/or becomes the basis for [7].

Once again the following precepts are offered:

- All staff and students making use of social media should try to be cognisant of the persistence, replicability and visibility of any comments or content they add on social media sites and, as appropriate, take care not to share any confidential or proprietary information.
- Where one's identity as an employee of the institute has been made explicit, that one's own personal views, where possible, should be distinguished from those of the institute.

In addition, it is suggested that:

- In cases where opinion is being offered with regard to the work of others that staff should take care – any in the context of the persistence and visibility of such comments – not to post anything defamatory or libellous.
- That staff should be aware of the need to respect copyright, intellectual property and confidentiality with regard to one's own work and practices, the work and practices of colleagues, and the work and practices of third parties. Such things are always important but perhaps doubly so in the online environment where everything is, so to speak, on the permanent (and imminently findable) record.

7. Students and staff sharing social media spaces for academic purposes

Social media has tremendous and, arguably, as yet untapped potential as a tool for teaching and learning. Academic and other staff in this context are encouraged to experiment and innovate in the use of a wide variety of social media spaces and services.

Certain guidelines from above carry through obviously, viz:

- All academic staff making use of social media should try to be cognisant of the persistence, replicability and visibility of any comments or content they add on social media sites and, as appropriate, take care not to share any confidential or proprietary information.
- Where one's identity as an employee of the institute has been made explicit, that one's own personal views, where possible, should be distinguished from those of the institute.
- In cases where opinion is being offered with regard to the work of others that staff, and students alike, should take care – any in the context of the persistence and visibility of such comments – not to post anything defamatory or libellous.
- That staff and students should be aware of the need to respect copyright, intellectual property and confidentiality with regard to one's own work and practices, the work and practices of other staff in the institute, and the work and practices of third parties.

In addition the following advice is offered:

- That staff try to act in keeping with the usual rules for engagement between staff and students apply in the online world. This means staff need to act in a way that is mindful of student rights and freedoms and to take care with comments and content which could be

interpreted as being discriminatory against any individual with regard to e.g. sex, race, sexual orientation, disability, religion, age etc.

- In addition staff need to be aware of their digital footprint and of the collapsing of the public and private sphere which this may entail. Staff, as appropriate, should endeavour to protect this distinction and moreover allow students the opportunity to do the same.

8. Official CIT Social Media Channels.

At present this is primarily the official Facebook page and Twitter account. Existing *Social Media Management Policy and Moderator Guidelines* apply here.