UNIVERSITY COLLEGE CORK

Acceptable Usage Policy

Version 1

2/1/2013

This document is designed to help the UCC community to understand their responsibilities when utilising, accessing or creating content with UCC's IT resources or networked services. It clarifies and defines (within reason) what the Universities deems as an acceptable use of these resources

Document Location

http://www.ucc.ie/en/it-policies/policies

Revision History

Date of this revision: 01/02/2013	Date of next review: 01/02/2014

Version Number/Revision Number	Revision Date	Summary of Changes
0.1	18/09/2012	Draft received from OCLA
0.2	9/10/2012	Draft updated in newly approved format and suggestions accepted
0.3	20/11/2012	Submitting to the IS&ER policy committee for approval
0.4	22/11/2012	Included website policy and communication policy. Also including suggestions from OCLA.
0.5	24/11/12	Edited to reflect suggested edits my John McNulty
0.6	25/11/12	John Morrison feedback edits
0.7	30/11/12	Final rebranding and edits
0.8	20/12/12	Feedback from IS&ER on enhancements to clarity
0.9	10/1/13	Approval by IS&ERC and final clarification amendments
0.11	17/1/13	Amendment's from Academic Board
0.12	1/02/13	Amendment's from Academic Council

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date
Gerard Culley	Director of Information Technology	06/11/2012
John Fitzgerald	Director of Information Services	06/11/2012
John Morrison	Chair of IS&ER committee	10/1/2013
Michael Farrell	Corporate Secretary	6/11/2012
Academic Council		01/02/2013

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

Table of Contents

1 Purpose 3
2 Scope 3
3 Supporting Policies, Standards & Procedures 4
4 Acceptable Use 4
4.1 Monitoring 5
5 Communication Systems 5
5.1 Passwords and Access 6
5.2 Security 6
5.3 Staff and Student/Alumni E-Mail 6
5.4 Internet 8
6 Personal Websites 8
6.1 Introduction 8
6.2 No use of University trademarks or logos without consent 9
6.3 Disclaimer 9
6.4 Limitations on Uses of Personal Websites 9
6.5 Removal of Websites 10
7 Breach of Policy 10
8 Revisions to Policy 10

1 Purpose

Providing an efficient and reliable computing and networking service, as well as access to communications devices, to staff, students and alumni depends on the cooperation of all users. It is therefore important that you are aware of your responsibilities. By using any of University College Cork – National University of Ireland, Cork (the "**University**")'s IT Resources (as defined below), you agree to comply with the terms of this Acceptable Usage Policy (the "AUP **Policy**"). This policy is without prejudice to the right to privacy as protected by the constitution and the European convention on human rights.

2 Scope

This AUP Policy covers documentation of policy, procedures and standards relating to:

- University College Cork Information Assets
- University College Cork IT Resources

This Policy applies to Staff, Students and/or External Parties (each of which is defined below") using the University's IT resources (which includes, without limitation, its networks (regardless of whether they are accessed remotely) and/or communications devices) (the "**University's IT Resources**")

University IT resources include those provided centrally by the University's IT Services as well as those provided locally in its offices, departments, schools, colleges or other units including, University IT resources accessed remotely via home working without limitation:.

(a) The University's network and connected networks and to all equipment connected to those networks physically or via wireless.

(b) Any networks created independently of the campus network, if they are connected to the University network.

(c) All University -owned IT equipment including servers, desktops, laptops, Personal Digital Assistance (PDA) and other mobile devices, network-related equipment; and

(d) Any equipment owned by third parties, leased or personally-owned which use the University network, in conjunction with their work or study in the University.

For the purposes of this AUP Policy:

- Staff means all full-time and part-time employees of the University, including research staff funded externally.
- Student means all full-time and part-time students of the University.
- External Parties means all the University's subsidiary companies, contractors, researchers, visitors and/or any other parties who have access to the University's IT Resources.

Here after, collectively referred to as "**Users**".

3 Supporting Policies, Standards & Procedures

Please note that certain additional standards and policies may supplement this AUP Policy in particular circumstances and therefore they should be read in conjunction with this Policy and all Users should ensure they are compliant with them. These are http://www.ucc.ie/en/it-policies

- Social Media Policy (available at: http://www.ucc.ie/en/media/support/itpolicies/policies/SocialMediaPolicy.pdf
- Unsolicited Bulk E-Mail Standards (available at: http://www.ucc.ie/en/media/support/itpolicies/standards/BulkEmailStandards.pdf
- Privacy Statement (available at: http://www.ucc.ie/en/media/support/itpolicies/PrivacyStatement.pdf
- Data Protection Policy (available at: http://www.ucc.ie/en/it-policies/pending-approval
- Digital Estate Governance Procedures (Available at: http://www.ucc.ie/en/media/support/itpolicies/draft/DigitalEstateGovernancePolicy(4).pdf

4 Acceptable Use

You must use the University's IT 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 AUP Policy, you must :

a) Not send unsolicited bulk e-mail (SPAM) or engage in any or other activities which are liable to cause a disruption or denial of service to other users. See bulk email standards for more details.
b) other than in the course of performing your duties, must not use computer or network resources to knowingly access or distribute illegal or inappropriate material, including material that is in any way pornographic, obscene, abusive, racist, libellous, defamatory or threatening;
c) Not engage in any form of bullying or other behaviour which is illegal or likely to cause harassment to others.
d) Not use social media to degrade, bully or intentionally offend staff or students of the University or use these tools to bring the reputation of the University into disrepute. Please reference the University's Social Media policy for more information
e) Not use computer or network resources for the purpose of gaining unauthorised access to the account, systems or equipment of any third party - attempts at 'hacking' may result in criminal prosecution in Ireland or elsewhere;
f) Not use computer or network resources for any activities which contravene the laws of the State, or the destination country in the case of data being transmitted abroad;
g) Not use computer or network resources for commercial activities or to otherwise further commercial objectives which are not a part of your work/studies in the University;
h) Not infringe the copyright, patent or other intellectual property rights of any person including, by downloading unlicensed software or other unauthorised materials;

i) Not share user IDs or usernames, transfer them to other users, divulge your passwords to other users, seek to impersonate other users or leave your computer unattended, even for a short period of time, without logging out or locking out as appropriate;
j) Not infringe the data protection or other privacy rights of any person;
k) Not access, modify, or interfere with computer material, data, displays, or storage media belonging to the University or another user, except with their permission;
l) Not knowingly introduce any virus, malware or other destructive program or device into the University's systems or network and you should take all reasonable steps to ensure that you do not inadvertently introduce such programs or devices into the systems or network
m) Not connect unauthorised equipment to the University network.

Where you access chargeable services (e.g. commercial online databases) and/or other electronic resources made available by the University's Library, you and/or your department may be liable for any charges incurred and you must follow any rules or guidelines in relation relating to their use.

If you process (or intend processing) personal data about others on a computer, you will need to comply with the provisions of the Data Protection Acts 1988 and 2003 as amended, updated or replaced from time to time.

4.1 Monitoring

Network traffic is monitored in circumstances where there is reason to suspect that this AUP is being breached, for the purposes of back-up and problem solving or where the University has other legitimate reasons for doing so. You must therefore be aware that such monitoring is taking place.

5 Communication Systems

The University IT resources are to support the activities of the University. Although limited personal use of the University's IT Resources is allowed, subject to the restrictions outlined below, no use of should ever conflict with the primary business purpose for which they have been provided, with the University's responsibilities or applicable laws and regulations. Each User is personally responsible for ensuring that the terms of this Policy are followed.

Data in the University's systems (including documents, other electronic files, e-mail and recorded voicemail messages) is normally considered the property of the University, 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. The University may inspect and monitor such data at any time where there is reason to suspect that this AUP Policy is being breached, for the purposes of backup and problem solving or where there are other legitimate reasons for doing so. The University may also monitor in circumstances where it is required to do so by law. Therefore, no individual should have any expectation of privacy for messages or other data recorded in the University's systems. This includes documents or messages marked "private", which may be inaccessible to most users. Likewise, the deletion of a document or message may not prevent the University from subsequently accessing the item in question.

5.1 Passwords and Access

The following activities, which present security risks, must be avoided by all Users.

- Attempts should not be made to by-pass or render ineffective security measures provided by the University.
- User Passwords must not be shared between users, except where they are released as part the approved procedure. If written down, passwords should be kept in locked drawers or other places not easily accessible. An approved procedure exists for releasing passwords where accounts are required and staff are unavailable, "Procedure Relating to Access by or Disclosure to a Third Party of Information in a Staff Member's Files or Email Account" http://www.ucc.ie/en/media/support/itpolicies/procedures/AccessToStaffAccounts.pdf.
- Document libraries, folders or files of other users should not be browsed unless there is a legitimate reason to do so and they are granted permission to do so. In some cases these document libraries may have general passwords, which should not be shared without the prior consent of the owner of the data in the folders (example: access to Academic Council papers must be approved by the registrar).
- The University's computer facilities should not be used to attempt to gain unauthorised access to or use of other computer systems or data.
- Unlicensed software or other material should not be loaded or executed on the University's equipment where this is likely to breach the licensing conditions or other intellectual property rights.

5.2 Security

There are a number of practices which individual users should adopt that will foster a higher level of security. Among them are the following:-

a) Disconnect your personal computer when you leave your work area or office for an extended period of time.
b) Ensure that you log-out when leaving your computer unattended even for a short period of time.
c) Exercise judgment in assigning an appropriate level of security to documents stored on the University's networks, based on a realistic appraisal of the need for confidentiality or privacy.
d) Back up any information stored locally on your PC (other than network based software and documents) on a frequent and regular basis.

5.3 Staff and Student/Alumni E-Mail

Each staff member within the University is provided with an email account to assist with their work for the University. Each registered student and graduate of the University is provided with an email account for their use, graduates and alumni are encouraged to keep this email for life. This account is the primary way that the University will use to communicate with students past and present. 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 University. In general, the University will respect the privacy of a staff member's email account. However,

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

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

Usage of the email system for academic and professional purposes is encouraged (journals, review papers, professional bodies, etc). 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 University or its business is not allowed. Personal use of e-mail is also subject to the same policies and regulations as official use.

Email held on central servers is backed up centrally on a three-week cycle to ensure system reliability and not for archiving purposes.

All email messages may be subject to the Freedom of Information Acts 1997 and 2003 (as amended, updated or replaced from time to time).

Arising out of the need to protect the University's network, the University cannot guarantee the confidentiality of information stored on any network device belonging to the University.

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

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 whether in written form, in cartoon form or otherwise, is strictly prohibited.

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.

If you receive any offensive, unpleasant, harassing or intimidating messages via e-mail, you are requested to inform the University immediately using helpdesk@ucc.ie .

You 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.

While messages should be accessed only by the intended recipient or delegates, the University 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 to external non-university accounts without prior approval from the Office of Corporate and Legal Affairs.

5.4 Internet

The University's Internet connections are intended for activities associated with the functions of the University, the exercise by staff of their responsibilities and duties and the professional/academic development of staff and students. The use of the University's systems for incidental personal purposes is permitted provided such use is in accordance with this policy, does not interfere with University operation of information technologies or electronic mail services, burden the University with incremental costs, or interfere with the user's employment or other obligations to the University.

Internet usage is monitored on a systematic basis by the University where there is reason to suspect that this AUP Policy is being breached and also for the purpose of back-up and/or problem solving or where there are other legitimate reasons for doing so. Internet usage may also be monitored by the University when it is required to do so by law.

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 University or the University's staff or students to others and/or to send other confidential information without approval;
e) when it interferes with your responsibilities; or

6 Personal Websites

6.1 Introduction

The University recognises that from time to time staff or students of the University will setup websites, blogs or wikis that while related to their academic or professional disciplines are personal sites and not formal University sites. This section of the Acceptable Usage Policy provides some rules around the establishment and usage of such sites. The purpose of these rules is to strike the appropriate balance of providing colleagues with the academic freedom to engage in open discourse, while also protecting the reputation of the University and that of its staff and students. In addition, this ensures that the individual views and opinions discussed openly on such sites are not portrayed as the formal position of the University.

6.2 No use of University trademarks or logos without consent

Personal websites should not display the University crest, logo or other University trademarked/copyrighted materials, including the University designs, or otherwise appear to be an official University web page, unless with the permission of the Office of Corporate and Legal Affairs.

Personal websites must not be used for commercial purposes in a way which conflicts with the Policy on Conflict of Commitment and Interest
http://www.ucc.ie/research/rio/pdf/Policies/CONFLICT%20OF%20INTEREST.pdf

6.3 Disclaimer

On personal websites, you are required to identify views expressed as your own and do not hold yourself out as representing the University. If you identify yourself as being a member of staff of the University, make clear that any views expressed are not necessarily those of the University.

Accordingly, all personal websites created and placed on the University's web servers and/or displaying University or copyrighted material shall include the creator's name, and on each page the following statement: 'A disclaimer applies to this page'. The word 'disclaimer' in the statement shall be a link to the following disclaimer:

*"This website is the personal responsibility of the person named in the website. Statements made and opinions expressed on personal websites are strictly those of the authors and not University College Cork – National College of Ireland, Cork ("**THE UNIVERSITY**"). THE UNIVERSITY does not preview, monitor, approve or endorse the contents of personal websites, and does not accept responsibility for any loss, damage, harm or injury occasioned by the contents of such websites including, without limitation, content which may be unlawful, offensive, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, discriminatory, libellous, invasive of another's privacy, hateful or racially, ethnically or otherwise objectionable material or content which otherwise infringes the rights of any third party on any personal page. THE UNIVERSITY is not responsible for the material contained in, or links connected to, personal websites and cannot be held liable for their contents."*

6.4 Limitations on Uses of Personal Websites

The use of personal websites for the following purposes is strictly prohibited:

a) any use which may have the effect of violating any laws (or exposing the University to unacceptable legal risk);
b) any use which may adversely impact on University computing or on network resources;
c) any use which the University considers may be defamatory or libellous;
d) any use which may infringe the rights of any third party in respect of personal data, intellectual property or other confidential or proprietary information;
e) making accessible materials which could have the effect of damaging the reputation and goodwill of the University;
f) Are otherwise in breach of this Policy.

These provisions are not intended to curtail normal academic discourse as guaranteed by S14 of the Universities Act 1997, but to provide an appropriate platform for this discourse that complies with the law of the land and one which does not damage the University or other parties.

6.5 Removal of Websites

The University reserves the right to remove personal websites (or links to externally located personal websites) when the limitations set out in section 6.4 above are breached or where the staff member resigns, retires or a student graduate or leaves.

Decisions regarding the removal of personal websites and/or links to externally located personal websites for any reason will be made by the web working group, who can be contacted at wwg@ucc.ie for more information please refer to the Digital Estate Governance procedure referenced in section three. Where urgent action is required in relation to a personal website or associated links (e.g. in the event of breach of this Policy) and it is not possible to consult the Digital Estate Governance team in the time available, then the Chairperson of the Committee or his/her nominee can decide on the action to be taken. The decision must be ratified by the Committee at the earliest opportunity, where the decision is not ratified, then the situation must be restored as closely as possible to that which existed before the action was taken.

7 Breach of Policy

The University operates a strict “notice and takedown” procedure. Users are encouraged to be vigilant and to report any suspected violations of this AUP Policy immediately to staffithelpdesk@ucc.ie On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this AUP Policy, the University reserves the following rights:

- To remove, or require the removal of, any content which is deemed by the University to be in breach or potentially in breach of this AUP Policy; and/or

To disable any User and access to the University’s IT Resources. If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

Revisions to Policy

The University reserves the right at any time to revise the terms of this AUP Policy. Any such revisions will be noted in the revision history of the policy, which are available to you on the website and by continuing to use the University’s IT Resources following any updated you will be deemed to have accepted the revised terms of this Policy.

8 Further Information

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

Director of IT Services

University College Cork

Tel: 021 4902215

Email: it_director@ucc.ie