Electronic Information and Communication Technology Policy and Procedures

September 2004

University College Dublin

Document Ref:	EICTPP
Version:	2.0 - September 2004
Original version:	1.0 - November 2002

CONTENTS

Electronic Information and Communication Technology Policy and Procedures

1.0 Introduction and Scope

University College Dublin is committed to providing computing resources including e-mail and internet access, for staff and student use to promote the aims of the University and to facilitate education, research and administration. This document constitutes University College Dublin's policies and procedures for the management of all aspects of electronic information and communication utilising the University's Electronic Information and Communication Technologies (EICT) infrastructure.

These policies reflect the ethical principles of the University community and outline the responsibilities of those using EICT services. The overall policy framework is "The Computer Network and Systems Acceptable Use Policy" which was approved by the President in September 2001 and contained in Section 2 of this document. The procedures reflect the implementation of that policy and related legislation and policies including the HEAnet Acceptable Use Policy with which the University must comply (Appendix 1).

This document applies to all aspects of EICT services at University College Dublin. These include the following:

. • WWW Publishing (all publishing under the .ucd.ie domain.)
. • E-mail and Electronic Communication.
. • Internet Accessible Servers - Security Service.
. • Discussion Groups.
. • Software and electronic library resources.
. • Technology and computing resources.

All individuals using any of the University's EICT Services, including those with their own equipment connected to the University's network, are required to abide by the terms of the "Computer and Network Systems Acceptable Use Policy" and any other procedures in this document which may apply.

The Computing Services Board has been designated by the President as the body responsible for implementing these policies.

This document will be revised to include relevant procedures for the provision of other services as they become available. The focus of this document is on the correct and appropriate use of these services.

The effectiveness of this Electronic Information and Communication Policy and Procedures will be reviewed by the Computing Services Board and relevant service providers on a regular basis (at least annually) and amendments made as required.

2.0 Computer Network and Systems Acceptable Use Policy

This policy was created by a nominated group established by the President and approved in September 2001.

2.1 University College Dublin is committed to providing computing resources, including e-mail and internet access, for staff and student use to promote the aims of the University and to facilitate education, research and administration.

To safeguard individual users and to ensure the integrity and reliability of the computer system, UCD has approved the following usage policies. These are not intended to limit an individual's use of the University's computer resources, rather they are designed to ensure that the University can offer the widest possible range of services to its community. Nothing that follows in this document attempts to limit academic freedom as set out in the Universities Act 1997.

The University is committed to maintaining the privacy of its users and does not actively monitor computer usage (including e-mail and the internet). However users should be aware that records are kept of all usage and could be made available in specific circumstances.

In general, the computer resources of the University may not be used for illegal acts, for activities in breach of University policies, for activities in breach of software or electronic library licences, or for personal commercial activity unless specifically authorised. Only staff of the University, registered students or other approved users may make use of the University's computer resources. Unauthorised use may lead to prosecution under the Criminal Damages Act 1991.

The following highlight a number of areas that you, as a user, must pay particular attention to.

2.2 You must respect the laws of Ireland and specifically, but not exclusively, be aware of your responsibilities under -

Copyright and Related Rights Act 2000
Criminal Damages Act 1991
Data Protection Act 1988
E - Commerce Act 2000
Prohibition of Incitement to Hatred Act 1989
Freedom of Information Act 1997
Child Trafficking and Pornography Act 1998

2.3 You may be provided with accounts and passwords to permit access to the university networks and other computer resources. You must take reasonable precautions to prevent unauthorised use of such accounts. In addition, if you are a staff member, you must ensure, in so far as practicable, that the computers in your office or under your control are not used for unauthorised purposes. Advice and practical help will be available to help you safeguard any computer equipment.

2.4 You must behave reasonably in your use of the university computer resources. You must not undertake or facilitate any activity that could jeopardise in any way, the integrity, reliability and performance of these resources. Any devices connected to the network must comply with the requirements of Computing Services. Check with Computing Services before you do anything that might affect the network. Wilful damage (or attempted damage) to computer resources will result in disciplinary action which may include prosecution under appropriate legislation. Likewise deliberately wasteful use of resources and time could lead to a withdrawal of services or severe disciplinary action.

2.5 You must take reasonable care to ensure that you do not transmit viruses or other malicious computer code to other users. The University will provide guidelines and practical help to all users to protect their computers.

2.6 It is not acceptable to view, download, transmit or store any offensive, indecent images or material. Nor is it acceptable to attempt to access any files, data or records for which you are not authorised. You may not use the University's computer systems to publish or transmit anything that is libellous or defamatory or is damaging to another computer system. Neither may you deliberately misrepresent your views as those of the University or any other person or organisation. Such action will be regarded as a serious disciplinary matter.

2.7 All software installed and used on the University's computer systems, including stand-alone computers, must be appropriately licensed. Where University site licences permit off-campus use and/or personal use, users must adhere to the terms and conditions of such licences.

2.8 Increasing amounts of data and information are stored on electronic media on the University's computer system. If you have access to, or are responsible for, such data you must ensure that the integrity, accessibility, accuracy and confidentially of such data are maintained. If you keep personal data on others you must comply with the provisions of the Data Protection Act 1988. You must also be aware that The Freedom of Information Act applies to records held in electronic format.

2.9 Failure to abide by these policies may result in being denied access to computer resources as well as other disciplinary proceedings.

This policy on acceptable computer use supersedes all previous policies on acceptable computer use and will be amended from time to time as required. Any user of University computer resources is deemed to have made him/herself aware of these policies.

3.0 Definitions relating to EICT Procedures

Electronic Information and Communication Technology Services

These are any services provided via the University's IT systems e.g. email, web publishing, FTP etc.

Registered Users

These are any members of the University Community entitled to an account on the University Computer Network. These will include academic staff, administrative staff, students and other users who have been authorised for access.

Campus Companies

Campus companies are those officially registered with the University Industry Programme. They are entitled to use UCD's EICT Services, in accordance with these policies and procedures.

University WWW Server

This is the main University WWW Server which hosts web accounts for colleges, schools, research groups etc.

Independent Servers

These are servers operated by some schools or research groups independently of Computing Services but which are registered on the University Computer Network. These will include servers that are accessible from the Internet.

Information Providers

A University club, society, school, college or other organisation registered to publish information under the ucd.ie domain. Information providers are responsible through their designated agents for the management and control of their WWW pages.

WWW Account

This is an allocation of space with password access and unique URL on the main University Server to an information provider. Typically an account will have between 5 - 20 megabytes depending on requirements.

WWW Pages

A single file, which can be linked through the use of hypertext with other files. A collection of WWW pages constitutes a WWW Site. The registered owner of the computer hosting the web site or the account holder (for main University Server) will be considered as the information provider/responsible person.

Designated Agent
Individuals designated by the information provider to take responsibility for the content and correct publishing of all pages on behalf of the information provider.

Domain Name/Sub - Domain
This is the top-level URL for the University e.g. ucd.ie. Schools operating their web site from an independent school server will have their own sub - domain e.g. chemistry.ucd.ie

Electronic library resources
Electronic databases, publications and other information resources licensed to UCD for the use of its staff, students and other authorised users.

4.0 Relevant Legislation

4.1 Data Protection 1988

Personal details held on computer may be subject to the Data Protection Act 1988. Users who maintain details of others on computer must make themselves aware of their obligations under the Data Protection Act 1988 and the Data Protection Directive (95/46/EC). This legislation confers considerable rights on individuals to control how data relating to them personally is stored and processed. In brief, personal data must be processed fairly and lawfully, it must be collected for specified, explicit and legitimate proposes and must be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed. Data may only be processed when the subject of the data has clearly given his/her consent for this to occur.

4.2 Copyright and Related Rights Act 2000

The wide accessibility of data networks makes it very easy to publish material electronically. Original information or data available on electronic bulletin boards, newsgroups, information services, on the WWW or by anonymous ftp, is copyright protected.

The Copyright and Related Rights Act 2000 updates existing legislation in line with technological developments and recent EU directives. For the first time, it includes explicit reference to publication in electronic form and to Internet publishing. Care should be taken to ensure that copyright material in any format is only used in accordance with the provisions of the Act, or with the permission of the copyright owner. This applies to all works - literary, dramatic, musical or artistic including original databases and computer software, as well as films, sound recordings, broadcasts, cable programmes, typographic arrangements, any computer generated works and any published editions. It also applies even where copies of copyright material are made available to UCD users only.

4.3 E-Commerce Act 2000

This Act is designed to clarify the issue of legal liability for Information Service Providers (ISP's) and therefore promote the growth of e-commerce unhindered by the weight of any legal uncertainty.

While this act was introduced to clarify the legal position for ISP's it also addresses some key issues which have relevance to WWW publishing in a University environment.

In relation to information for which the University does not take editorial control it is acting in the same role of an Internet Service Provider. As an ISP under this legislation there is no onus on the University to monitor the information it transmits or stores nor a general obligation to actively seek facts or circumstances indicating illegal activity.

However, based on this legislation it is clear that the University does have a legal responsibility to act expeditiously to remove or to bar access to information upon request by the relevant legal authorities or when the University is made aware that defamatory or other illegal materials are being published.

These policies have been adopted to ensure that the University is in compliance with the principle of this legislation.

The University reserves the right to monitor any Internet communication as outlined on section 2.0 on Acceptable Use.

4.4 Child Trafficking and Pornography Act 1998

This Act was introduced to strengthen legislation to prohibit trafficking in, or the use of, children for the purposes of their sexual exploitation and the production, dissemination, handling or possession of child pornography, and to provide for other related matters.

4.5 Criminal Damages Act 1991

This Act includes provisions which make it a criminal offence to wilfully damage property or data. It prohibits the destruction, defacement, dismantling - temporary or otherwise - of a person's property. In relation to data it makes it an offence to alter, corrupt, erase or move to a different location or storage medium. Property under the terms of this legislation is defined as something belonging to another person.

4.6 Prohibition of Incitement to Hatred Act 1989

The Incitement to Hatred Act 1989 prohibits the publishing, broadcasting or distribution on any material which would incite hatred on the grounds of race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation.

4.7 Freedom of Information Act 1997

The Freedom of Information (FOI) Act 1997 asserts the right of members of the public to obtain access to official information to the greatest extent possible consistent with the public interest and the right to privacy. The University came under the scope of this legislation on 22 October 2001.

The Act establishes three new statutory rights:

- a legal right for each person to access information held by public bodies.
- a legal right for each person to have official information relating to him/herself amended where it is incomplete, incorrect or misleading.
- a legal right to obtain reasons for decisions affecting oneself.

In addition, the Act provides for the establishment of an independent Office of Information Commissioner to review decisions relating to FOI made by public bodies.

For further information on the Freedom of Information Act and its application at UCD please visit the UCD Freedom of Information Office Web Site at http://www.ucd.ie/~foi

5.0 Procedures for Use of EICT Services

5.1 Introduction

Registered users are entitled to use the University's EICT Services free of charge for their academic requirements. The usage of the EICT Services is dependent on the agreement of the user to follow these regulations and by the agreement of the user to respect the rights and privacy of all other users. Registered users formally agree to these regulations when they apply for:

? A Computer Account (Access to the UCD Network)
? To have a machine registered for access to the UCD Network
? WWW Publishing Account

Infringements of these regulations will give rise to sanctions and penalties as laid down in the staff and student disciplinary procedures (Section 10).

Registration procedures for these services can be found on http://www.ucd.ie/itservices

5.2 Network Access Procedures

Staff and students are entitled to connect personal computers to the University network where such a connection has been registered. Registering for a connection is done through the Computing Services website http://www.ucd.ie/itservices/machinereg

5.2.1 Network Zoning

The UCD network is divided into a number of zones, each with different access levels and appropriate uses. Each building has a separate virtual network to isolate its activity and prevent major campus wide outages.

Within each building there are in general four zones:

- private cabled zone (in secure staff offices)
- public cabled zone (in labs or accessible offices / spaces)
- administrative zone (in certain buildings & large admin offices)
- wireless zone (where provided)

Different levels of service and protection are provided in each of these zones, and on the basis of client or server status of computer equipment.

5.2.2 Network Account Registration

To access the network it will be necessary to obtain a UCD network account (i.e. existing UCD login ID, or UCD Connect account). All users accessing the network will be required to authenticate on connection using this login.

5.2.3 Laptop/Desktop Registration

In addition, desktop or laptop equipment connecting to the cabled network must be registered with Computing Services.
http://www.ucd.ie/itservices/accountrequest

5.2.3.1 Configuration

Desktop or laptop client equipment must be configured to use DHCP, and should not under any circumstances use fixed IP addresses. Computing Services **do not** allocate a specific address to client equipment.

5.2.4 Server Registration

Specific provision is made for **servers** in Colleges, Schools or belonging individual staff users. Where equipment provides a published service, the UCD staff member responsible for the equipment, must register the server with Computing Services. The server is then allocated a fixed DNS name and IP address, which is accessible on or off campus. Server registration will be confirmed on an annual basis. The staff member is responsible for securing the equipment, ensuring that use complies with UCD policy, and that the server does not impact on general network or IT performance.

5.2.4.1 Server Security

Procedures for setting up servers are available on the Computing Services web site at http://www.ucd.ie/itservices/serversecurity

5.2.5 Network Management

The UCD network is managed and maintained by Computing Services. No network equipment, wireless equipment, or software which simulates network equipment (e.g. bridging) may be connected or installed without explicit written agreement from Computing Services. Unauthorised equipment may be disconnected from the network. (An open research network zone may be provided for experimental purposes in selected locations).

5.2.6 Wireless Frequency

In order to ensure the provision of acceptable levels of service to the UCD community, WLANs can only be set up with prior authorization and agreement. UCD Computing Services has local authority for the installation and operation of WLAN equipment, WLANs operating outside of this remit may be removed from the network.

5.3 Security Management Procedures

In order to provide the highest level of security on the UCD network, Computing Services provides the following security service:

- On-line registration for servers that are accessible from the internet.
- Information pages on the Computing Services WWW site that give clear information on how to secure a server.
- Information pages on the Computing Services WWW site that post security vulnerabilities and patches relating to server software.
- A security e-mail list that provides messages on new information posted to the security web pages.

Information on the above services can be found on
http://www.ucd.ie/ itservices/serversecurity

5.3.1 Server Equipment

All server equipment must be registered by the owner responsible with Computing Services, and renewed on a periodic basis. Administrators of servers must ensure they are fully aware of security requirements, and manage their equipment accordingly. Equipment which is not secure or which compromises performance may be removed from the network. Computing Services provides security on the network and for centrally managed servers, security for Individual, College and School servers is the responsibility of their registered owners. Computing Services provides software, services advice and support to users in maintaining a secure environment.

5.3.2 Individual Computer Equipment

Computing Services licences and provides virus protection software for all staff and students, including automated updates. Virus protection and update services should/must be installed on all equipment connected to the UCD network. Security advice and support is available on our web site for both desktops and servers www.ucd.ieitservices/desktopsecurity and www.ucd.ie/itservices All equipment should have an up to date Operating System and relevant software patches installed. All equipment and accounts should be protected by a secure password.

It is the responsibility of staff and students to ensure their equipment is adequately secure by availing of these services. Equipment which is not secure or which has been compromised may be removed from the network. Computing Services routinely scan the network and equipment to ensure adequate security and performance.

5.3.3 Laptop Procedures

Computing Services supports the connection of approved laptop equipment to the UCD network. A contract is negotiated annually with suppliers for products and software, including hardware support and maintenance. All such equipment is purchased directly by staff /schools or students from the supplier, hardware support and maintenance is the supplier responsibility.

Computing Services provides support in connecting to the network, user network accounts and equipment registration. Different levels of service are available according to the network zone.

Cabled areas provides the highest quality of service and a range of applications. Wireless areas provide Web access and UCD email **only**, and in general are likely to have lower speed of access.

Where unapproved laptop equipment is used, Computing Services cannot guarantee service. If the equipment is registered and used with a valid network account, the user may configure to access the network and services.

All laptop equipment must be secured in accordance with security procedures.

5.4 Administrative Network Security Procedures

The administration network will be divided into 3 zones

- Administration server zone
- Administration building – user desktop zone
- Other Administration users network zone – e.g. in -Colleges / Schools

DHCP should be used by all desktop equipment in the Admin User zones. (The use of IP address as a means to restrict or secure access to systems is no longer used)

In general, user zones on the UCD network should be treated as a "public network" when considering the security of information or when allowing general access to systems or information, as physically securing access to the network on a campus wide basis is not possible. Appropriate authentication and security measures are described below.

5.4.1 Authentication

Network based authentication, which uses the core LDAP directory (NDS) will be introduced at connection point to the network. Where possible other systems should authenticate to the LDAP as the primary and comprehensive user directory. Application level authentication should be used to secure access to individual systems. Appropriate levels of login and / or information security and encryption should be defined and implemented. The UCD Connect environment provides an authenticated entry point (on & off campus) to the "UCD Intranet" and should be used where access to information or services needs to be restricted by role – e.g. staff / student etc.

5.4.2. Desktop Security

Administration desktops should at a minimum be secured in accordance with the general desktop / laptop security policy i.e. virus protection, OS updates, & secure passwords. It is recommended that a secure and protected build be installed for all administration desktops – both within central administration and in college offices.

6.0 Procedures for Protection of Privacy

All EICT Services are password protected and all passwords should be kept confidential. Registered users should make themselves aware of good practice when changing their passwords. Passwords should not be words which are in the dictionary or which relate to personal details. Composite words or passwords containing both letters and numbers are safer. Passwords should be longer than 6 characters.

All information held on computer is considered to be confidential unless obviously intended for unrestricted dissemination. No registered user should attempt to access information unless he or she has permission to do so.

Communications in transit on the Internet or University network are also confidential and unauthorised monitoring of any electronic communications is forbidden.

7.0 Procedures for WWW Publishing

7.1 Introduction

This section governs all aspects of WWW Publishing at UCD and the procedures are published and updated by the UCD WWW Committee.

All UCD organisations publishing information in the UCD domain (www.ucd.ie) are known as information providers and are obliged to make themselves aware of their obligations under these procedures.

The UCD President appointed the WWW Committee to work in co-operation with University information providers to ensure the maintenance of a high quality WWW presence which represents the full range of activities and services at UCD.

7.2 Applying for a WWW Account

All information providers opening an account on the main UCD server are required to complete a **WWW Account Application Form, -** http://www.ucd.ie/itservices/internet/webpublishing.htmltaking responsibility for their own published content. Information providers publishing from an independent WWW server connected to the UCD network should register in the normal way with Computing Services. The information provider is responsible for ensuring that all web publishing complies with these policies (Section 7.4.7).

On registration, a WWW Account will be set up on the main University WWW Server with 5/10 megabytes of space. This may be increased depending on requirements.

7.3 Termination of Accounts

Information providers should notify the WWW Editor when they no longer require their WWW publishing account or when any of the details submitted with the application change. Accounts that have not being renewed as part of the standard renewal procedure may be terminated. Accounts should be renewed on at least a bi-annual basis or in the case of schools on an annual basis.

7.4 Editorial Policies and Responsibilities

7.4.1 General

The WWW Committee has designated the Web Editor as the person to work with the University Community to ensure the correct implementation of these procedures. The Web Editor is available to advise on matters relating to WWW publishing. However, the WWW Committee or its designates undertake no editorial control of information published by information providers. Information providers through their own designated agents are responsible for any contravention of the law, which may be caused by the content of WWW pages under their control, under the legislation outlined in section 6.0.

7.4.2 Accessibility

University College Dublin is committed to a policy of access for all users of our WWW site including those with disabilities. In support of this policy UCD will strive to adhere to the accessibility standards published by the World Wide Web Consortium (W3C), WWW Content Accessibility Guidelines (http://www.w3.org/TR/WAI-WEBCONTENT/) in the preparation of digital content for the WWW.

Web design training programmes for site administrators will include training on best practice for accessibility. In addition, the administrators of new and existing web sites will be encouraged to seek the Centre for Applied Technology's "Bobby" standard for accessibility (http://www.cast.org/bobby/)

The UCD WWW Committee is committed to working with the University's Disability Support Service in the implementation of this policy.

7.4.3 College/ School Publishing

Each college is obliged to have a WWW site publishing a basic level of college information. Each college in turn is responsible for ensuring that each of their schools has a presence on the WWW.

The Head of School should approve the setting up of a school web account and may appoint a designated agent who will take responsibility for the day to day maintenance of the WWW account. Each college and school as a minimum should maintain a WWW presence linking to basic academic programme information published by the Admissions Office and the Postgraduate Studies Office. Each school will be required to renew their account on a regular basis. As a very last resort, schools that fail to renew their WWW account may have their WWW publishing account temporarily removed from the main UCD WWW server.

Online course material, for UCD programmes should be published through the University's supported Virtual Learning Environment.

7.4.4 Research or Inter-college Group/Centre Publishing

All official University Research Groups or Centres are editorially responsible for content published on their WWW sites. Each Group/Centre is responsible for their own published content. These accounts will also be renewed on a regular basis.

7.4.5 Staff Personal WWW Pages

Individual personal WWW pages should only be used to publish material, which relates to the activities and responsibilities of the staff member (e.g. academic profiles, research interests/ activities, publications etc.). These pages are the responsibility of the member of staff registered as the owner of the WWW account. Staff personal pages are to be published under the sub-domain **staff.ucd.ie.** when this becomes available. In the meantime, all staff personal content should be published from a directory within the school's web account. The Head of School should preferably nominate a person responsible for the administration of staff personal pages. Individuals publishing personal pages must undertake to comply with these policies and regulations.

7.4.6 Student WWW Publishing

Clubs and societies are encouraged to publish their own web sites and are supported by the University Web Unit.

Auditors and/or secretaries of clubs and societies are responsible for the information published on behalf of their club/society. All club and society WWW accounts must initially be approved by the Student Consultative Forum or designate at the beginning of each academic year. It is the responsibility of the incoming club/society committee to renew their account by completing the Club/Society **WWW Account Renewal Form** available from the Computing Services web site at http://www.ucd.ie/itservices/internet/webpublishing.html

Student personal WWW accounts are only permitted under the supervision and control of a course director or other academic supervisor who will be responsible for the material published in the student account. These "course work WWW publishing" accounts are published under a separate sub-domain, **www.weblab.ucd.ie.**
All other student WWW publishing accounts will be published under the **www.student.ucd.ie** sub-domain.

7.4.7 Information Provider (e.g. School) maintained servers

Other information providers operating from an independent school server but connected to the University network will come under their own sub-domain e.g. http://www.cs.ucd.ie for the School of Computer Science.

These information providers while not publishing material on the main UCD WWW server are still obliged to make themselves aware of their obligations under these EICT Policy and Procedures.

UCD schools publishing from their own servers are obliged to request an alias on the main University Server, so as to ensure consistency in URL structure for visitors to our site. e.g. www.schools.ucd.ie will also be available through www.ucd.ie/school

Schools operating independent servers should make themselves aware of the Internet Accessible Servers - Security Service operated by Computing Services (Section 5).

7.5 Administrative Procedures for Web Publishing

UCD has introduced standard corporate branding for college and administrative centre WWW pages which will allow scope for individual presentation by each college/administrative centre. Schools that do not follow this standard presentation should have a cover page hosted under the College WWW account which will serve as an introduction to the school's own WWW site.

It is important that appropriate care be taken in the presentation, content and management of information being published electronically by all information providers. This includes:

- Only the latest version of publications should appear on the WWW.
- Revision of publications should come from a single authoritative source.
- Information providers should implement procedures to ensure there is a match between electronic and hardcopy publications. Also, information providers are responsible for implementing procedures to ensure a match between academic programme content published in two locations e.g. School's web site and Postgraduate Studies web site.
- Care is to be taken in writing, proofing and layout.
- All information providers should adhere to WWW publishing guidelines that may be published from time to time in support of this policy.
- Information providers should notify the WWW Editor when they no longer require their WWW account.
- It is the responsibility of all information providers to ensure that all internal and external hyperlinks are working correctly.
- All information providers should be cognisant of the fact that many other information providers may have important links to their own site. This cross linking must be supported when redesigning file structures during WWW site upgrades.
- Information providers should use relative rather than absolute links where possible when constructing WWW sites. E.g. /news/story1.htm rather than http://www.ucd.ie/~accountname/news/story1.htm
- Schools that wish to host their own domain name e.g. www.chemistry.ie may do so external to the University or on their own school's server. These domain names should be secondary to the URL of their site hosted under the ucd .ie domain e.g. www.ucd.ie/chemistry. The formal UCD version of the URL should be the only version which is promoted on official school or programme literature.
- UCD WWW sites registered with external search engines and directories should be registered in such a way so as not to appear as the principal point of access to the University's main web site.

? All official University information e.g. programme information should only be published by the official channel for that information e.g. Admissions Office/Public Affairs/Registrars Office. Where this information is duplicated on a school web site it is the responsibility of the school to ensure they are publishing the correct and official version.
? Only official University organisations are permitted to use the University Crest. Organisations not officially members of the UCD Community are not permitted to use any UCD related material including graphics to falsely present themselves as having an official relationship with the University.

7.6 Procedures for WWW Site Content

7.6.1 Administrative Information – All UCD WWW Sites.

The content and structure of all registered WWW sites will vary depending on the specific requirements of each college/school. But there is a level of common administrative information which is important to include on all UCD WWW sites.

- The formal title of the organisation/college/school and an e-mail address for general enquiries.
- Date of last update on the site's homepage.
- E-mail address of responsible/designated person, for site specific enquiries and feedback.
- Approved standard legal disclaimer.
- To discourage copyright infringement, state the copyright symbol (©), year of production and the name of the copyright holder.
- Site navigation structure with, as a minimum, a hypertext link to the site's homepage on each page of the site, a link to office/school contact information and a link to the UCD Homepage. Full internal navigation structure should also be incorporated into the site design.
- Pages with scrolling information should have a link back to the top of the page.

7.6.2 School WWW Sites - Minimum Content

- Basic administrative content detailed in previous section.
- University crest should appear on the homepage and as part of overall site design.
- School name, location, contact number and generic email address to take the form e.g. schoolname@ucd.ie.
- Staff names, contact information (permission must be sought from each staff member before publishing this information.)
- Undergraduate programmes. Where appropriate links should be made to the Admissions Office at http://www.ucd.ie/~admiss.
- Postgraduate programmes. Where appropriate links should be made to the Postgraduate Studies Office at http://www.ucd.ie/~pgstudy.
- Schools may of course publish more detailed information on their WWW sites if they wish, than that published by the central University offices. (e.g. Admissions Office) but the official programme information must match that published by the Registrar's Office in the college booklets. These booklets are available online at http://www.ucd.ie/registrar

7.6.3 Standard Legal Disclaimers

A standard legal disclaimer should appear on all official University web sites. This disclaimer should be positioned so as to be readily viewable to the user.

The information contained in these WWW pages is, to the best of our knowledge, true and accurate at the time of publication, and is solely for informational purposes. University College Dublin accepts no liability for any loss or damage howsoever arising as a result of use of or reliance on this information, whether authorised or not. By continuing, I am accepting these conditions.

Information published by individuals should be declared as such and should not appear to be published on behalf of the University. There will be a clear distinction made between UCD information and personal information and the latter should contain the following disclaimer.

The views and opinions expressed in this page are strictly those of the page author. The content of this page has not been reviewed or approved by University College Dublin.

8.0 E- Mail Procedures and Guidelines

8.1 Introduction

The intent of these email guidelines is to make clear the appropriateness of certain uses of e-mail and while not being exhaustive it does detail the minimum standards required by users of the University's e-mail services. E-mail users should abide by the following guidelines in addition to the general acceptable use regulations (Section 2.0).

8.2 General University E-Mail Guidelines

- Registered Users should be aware that electronic mail, to from or within the University, may be the subject of a request under the Freedom of Information Act, 1997.
- E-mail accounts are backed up as a regular course of network operation. Deletion of e-mail messages does not remove all traces of the message.
- E-mail is not guaranteed to be private.
- The University is not liable for lost or deleted e-mail.
- Chain letters should never be sent through e-mail. Sending them may cause security and performance issues with the e-mail system.
- Be professional and careful what you say about others. E-mail is easily forwarded.
- Personal e-mail should not be forwarded to mailing lists or other users without the original author's permission.
- It is prohibited to send email with a hidden or false identity.

9.0 Procedures for Electronic Library Resources

The terms and conditions of licences governing the use of electronic library resources must be complied with.

Terms and conditions vary in their detail, but include the following:

9.1 Electronic library resources are licensed to UCD for the use of currently registered UCD staff and students and, only as provided for and defined by an individual licence, other authorised users.

9.2 Electronic library resources may be used for the purposes of UCD teaching, learning, research and administration only. They may not be used for commercial gain or for work undertaken by a student for the benefit of her/his employer. This includes the employer of a student on work placement as part of a UCD course.

9.3 Any copyright statement, proprietary marking, or protection measure included on any copy, or copies, derived from an electronic library resource must not be removed or interfered with.

9.4 Any copy, or copies, derived from an electronic library resource must be made within the terms of the licence. This will normally exclude the copying of the whole, or substantial part, of a database, journal issue or other publication.

Copies of licences for individual resources are available on request from the Library.

10.0 UCD Disciplinary Procedures

Breaches of this policy by staff or students are governed by the appropriate UCD disciplinary procedures namely:

I. The UCD Student Code and Student Information Handbook
II. Personnel Office Grievance and Disciplinary Procedures

Students who fail to observe the Electronic Information and Communication Technology Policy and Procedures may be subject to the following actions:

- Computer account may be suspended on a temporary basis or may have restrictions place upon it
- Access to computer facilities may be denied on a temporary basis or access may only be permitted under restrictions/conditions
- The student's head of school may be notified on the details of the student’s misuse
- A notification from the head of school may be required to reinstate services.

If appropriate, authorised users may have their access to UCD's computing facilities suspended pending an investigation by an authorised person in the University.

In the event of a loss being incurred by UCD as a result of a breach of this policy by any user of the computing facilities, that user may be held responsible for reimbursement of that loss.

Appendix

HEAnet Acceptable Usage Policy

Background and Definitions

1. HEAnet is the name given to the collection of networking services and facilities which support the communication requirements of the Irish education and research community.

2. HEAnet provides services to three categories of organisation - member, user and connected.

3. Member organisations are those organisations that have involvement in the management of HEAnet and form the Board of HEAnet. These are the seven Universities, the HEA, the ITs, DIT and the Government.

4. User organisations are those organisations that the Board has decided are eligible to subscribe for HEAnet services.

5. Connected organisations are those organisations that the Board has decided are eligible to connect to HEAnet. Such organisations are only allowed to connect to sites directly connected to HEAnet - i.e. they are not allowed to transit HEAnet into other networks.

6. This policy statement applies to all three categories of organisation. It is the responsibility of User Organisations to ensure that members of their own communities use HEAnet services in an acceptable manner and in accordance with current legislation.

7. Organisations using HEAnet should establish their own acceptable usage policies in a form that is compatible with the conditions expressed in this policy.

8. An organisation availing of HEAnet services is a user organisation. It is acceptable for a user organisation to extend access to others on a limited basis (subject to 9 below), provided no charge is made for such access.

9. A user organisation may provide HEAnet services to organisations which support the aims and objectives of HEAnet and which, in the opinion of the user organisation, have a contribution to make to the HEAnet community of members.

10. The HEAnet may provide services to third parties (not members of the HEAnet) provided that, in doing so, there is benefit to the membership of the HEAnet.

Acceptable Usage

HEAnet services should be used in such a way as to:

- apply public funding only to the purposes for which it was voted;
- abide by the law of the land;
- and not conflict with or override the rules and regulations of member organisations.

HEAnet will actively seek grants, subventions and other assistance towards its aims and objectives from public and private sources as appropriate.
A code of acceptable behaviour in the usage of HEAnet services is given in the Appendix .

Appendix: HEAnet Code of Behaviour

HEAnet provides enabling and enhancing services for member organisations in the pursuance of their official activities of instruction, research and development, and associated academic activities, and for administration in direct support of such use.

It is not permitted to use HEAnet services for any activity which purposely:

- seeks to gain unauthorised access to the resources of member organisations
- adversely affects the operation of HEAnet services or jeopardises the use or performance for other users
- wastes resources (people, capacity, computer)
- destroys the integrity of computer-based information
- compromises the privacy of users
- creates or transmits (other than for properly supervised and lawful research purposes) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- creates or transmits defamatory material
- transmits material in such a way as to infringe the copyright of another person or organisation
- transmits unsolicited commercial or advertising material
- causes offence or discriminates on grounds of race, creed or sex
- conflicts with practices as laid down from time by the Board
- contravenes the law of the State (in particular, but not exclusively, the Data Protection Act and the Criminal Damages Act(1991)).

It is the responsibility of user organisations to restrict traffic according to their own requirements and to secure themselves against the misuse of HEAnet services.

It is the responsibility of the user organisation to take all reasonable steps to ensure compliance with the conditions of acceptable usage and to ensure than unacceptable usage of HEAnet services does not occur. The discharge of this responsibility must include informing all users of HEAnet services of their obligations in this respect.

Where necessary, HEAnet service may be withdrawn from the user organisation. This may take one of two forms:

- An indefinite withdrawal of service, should a violation of these conditions persist after appropriate warnings have been given by HEAnet. Such a withdrawal of service would only be made on the authority of the Board. Restoration would be made only when the Board was satisfied that the appropriate steps had been taken at the organisation involved to ensure acceptable behaviour in future.
- A suspension of service, should a violation of these conditions cause serious degradation of the service to other users. Such a suspension would be made on the judgement of the Board, and service would be restored when the cause of the degradation of service to others had been removed.

The responsibility for interpreting these terms lies with the Board. The Board reserves the right to review these conditions from time to time.