UNIVERSITY OF GLOUCESTERSHIRE

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY FRAMEWORK OF DOCUMENTS

This Policy Framework covers the use of the Information and Communications Technology (ICT) in the University of Gloucestershire and consists of:

I. **University Network User Agreement** which specifies the general responsibilities and standards of conduct expected of a user.

II. **University Network Policy** which specifies the University's Policy regarding user responsibilities, general computing and the consequences of violation. Staff are issued with a copy of the framework which also forms part of the induction process.

III. **University E-Mail & Internet Use Policy** (Adapted to include the previous University Acceptable Use policy)

IV. **University Computer Hardware & Software Policy** that provides policy guidance on the type of hardware and software used in the University

V. **University Phone Policy** which specifies the policy and expected conduct of users of University phone systems.

VI. **University Information System Policy** which provides advice and guidance on the use, and purchase of, corporate information systems in the institution

Users who access electronic resources through a University account *(i.e. username/password)*, should familiarise themselves and comply with the content of this framework of policies.

UNIVERSITY OF GLOUCESTERSHIRE

UNIVERSITY NETWORK USER AGREEMENT

When a 'User' logs on to the network at the University of Gloucestershire they agree to adhere to the following guidelines.

1.0 General

You will :

1.1 be the sole person authorised to use this User ID;

1.2 be solely responsible for all actions taken under your User ID while it is valid;

1.3 not let others use your User ID and your Password nor inform others of your User ID or Password;

1.4 not delete, examine, copy or modify files and/or data belonging to other users without their prior consent;

1.5 not deliberately impede other users through mass consumption of system resources;

1.6 not take any unauthorised, deliberate action which damages or disrupts an ICT system, alters its normal performance, or causes it to malfunction, regardless of system location or time duration;

1.7 accept that, data stored on the Network can be moved internally by qualified staff in ICT Services.

2.0 Electronic Mail

You will :

2.1 be responsible for all electronic mail originating from your User ID;

2.2 not forge, or attempt to forge, electronic mail messages;

2.3 not attempt to read, delete, copy or modify the electronic mail directed to other users without prior consent;

2.4 not send, or attempt to send, harassing, obscene and/or other threatening e-mail to another user of any e-mail service. Further

information can be found in the University's E-Mail and Internet Policy;

2.5 not send 'for-profit' messages or chain letters.

Further information regarding the University E-Mail and Internet Policy which is detailed later in this document.

3.0 Network Security

You will not :

3.1 Use University Systems in an attempt to gain unauthorised access to remote systems;

3.2 attempt to gain unauthorised access to University Systems from remote systems;

3.3 attempt to decrypt the system or user passwords;

3.4 copy University System Files;

3.5 attempt to 'crash' University Systems or programs;

3.6 attempt to secure a level or privilege on University Systems higher than authorised;

3.7 load programs or computer software applications onto the University Systems or computer hard disk without the written authorisation of the ICT Manager;

3.8 wilfully introduce computer 'viruses' or other disruptive/destructive programs into the University Systems or into external networks.

3.9 use non-University ICT equipment on the Network.

4.0 ICT Policy Framework

The Framework requires that you:

4.1 are aware of the University Information and Communications Technology Policy Framework including all its constituent parts and accept its terms and conditions;

4.2 accept that violation, or attempted violation, of your responsibilities as a user may lead to your exclusion from the System;

4.3 have read and understood this User Agreement and accept full legal responsibility for all of the actions that you commit using the University's Systems according to any and all applicable laws;

4.4 understand that from time to time the University Systems and attached equipment may fail unexpectedly while you are using them and you will not hold the University responsible for lost time or data.

UNIVERSITY OF GLOUCESTERSHIRE

UNIVERSITY NETWORK POLICY

1.0 Statement

The Information and Communications Technology (ICT) belonging to the University of Gloucestershire is provided for use by students, University staff and contractors' staff in support of the vision and corporate objectives of the University; reasonable personal use is also acceptable, however users should be aware that the University cannot guarantee privacy of network traffic. All users are responsible for seeing that these technologies are used lawfully, ethically and courteously.

2.0 Responsibilities

2.1 The University is responsible for securing its facilities to a reasonable and economically feasible degree against unauthorised access and/or abuse. This responsibility includes informing users of expected standards of conduct and the resultant consequences for not adhering to them.

2.2 The users of the Network are responsible for respecting and adhering to Scottish, United Kingdom, European and International Law, the University's Internet Service Provider's Acceptable Use Policy, as well as the policies of the University.

2.3 Information and Communications Technology (ICT) can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, the integrity of the systems and related physical resources.

2.4 It is the policy of the University of Gloucestershire to respect all computer software copyrights and adhere to the Terms and Conditions of any licence to which the University is a party. The University will not condone the use of software that does not have a licence and any user found installing unlicensed software will be dealt with under the terms of the relevant Disciplinary Policy and Procedure.

2.5 The authoritative data source for the creation and deletion of Network accounts is the SITS system for student accounts, and the Human Resource System for staff accounts.

2.6 Only ICT equipment approved by ICT Services will be able to gain access to the University network.

3.0 General Computing Policy

3.1 Authorised users of University Network facilities shall be issued with a unique User ID.

3.2 Prior to using their unique User ID, users shall agree, through agreement on screen, to uphold the terms of this Policy Framework and its constituent parts.

3.3 Authorised users are solely responsible for all actions, including Electronic Messaging, taken while their User ID is in use. Authorised users are responsible for maintaining the confidentiality of their passwords and the security of their accounts.

3.4 Any graphics, multimedia programs, instructional material or articles produced wholly or in part using the University Systems remain the Copyright and intellectual property of the University of Gloucestershire.

3.5 The ICT Policy Framework may be amended from time to time as deemed appropriate by the University.

4.0 Measures

4.1 Any attempt to violate the provisions of this Policy, regardless of the success or failure of the attempt, will result in disciplinary action. Disciplinary actions may range from a reprimand, exclusion from the system or penalties afforded under University Policies. Disciplinary action in relation to staff will be in terms of the University Disciplinary Policy and Procedure, including summary dismissal where appropriate.

4.2 Any attempt to circumvent Scottish, United Kingdom, European or International Law through the use of University owned facilities may result in litigation against the offender by the appropriate authorities, If such an event should occur, the University will fully comply with authorities to provide any information necessary for the litigation process.

4.3 The University reserves the right to monitor use and to withdraw access from Users to all or part of its University Systems and other Information and Communication Technology at any time.

5.0 Rights of Appeal

5.1 The decision to exclude a user from University Systems will be made by the Head of Learning & Information Services (Strategy & Resources).

5.2 With reference to students, an appeal against the decision should be made using the procedures outlined in the University Student Appeals Procedure. The decision of the University Student Appeals Panel is final.

5.3 Staff should appeal using the University Grievance Policy and Procedure.

UNIVERSITY OF GLOUCESTERSHIRE

UNIVERSITY EMAIL & INTERNET POLICY

1. Scope

1.1 The aim of this policy is to provide guidance in the effective use of the University network to support the main business activities of the institution that include learning, teaching, research and administration. The policy has been developed to enable and encourage the exchange of electronic forms of information in a controlled and secure way.

1.2 The term network, and references to it throughout this document, covers the use of any local area network within the University, as well as access to the Internet and other networks using University equipment and the SuperJANet network.

1.3 The University connects to the Internet via the Higher Education SuperJANet network and is subject to the terms and conditions as set out in the SuperJANet acceptable use policy which can be found at: http://www.ja.net/services/publications/policy/aup.html

1.4 The SuperJANet Acceptable Use Policy (AUP) has the underlying principle that use of the educational network must be for 'legal, honest and decent' purposes. It is not provided for private business use by staff or students. All users are ultimately responsible for their actions when accessing networked services.

1.5 All staff, students and associate members of the University who have been granted authorised access to the University network, must abide by these policy rules and regulations and the terms and conditions set out Janet AUP.

Supplementary information regarding authorised access to the University network can be found in the University Network Policy detailed earlier in this document.

2. The Use of Computers at Work

2.1 The University's computers are provided to support learning, teaching, research and administrative activities in the institution. Access is only permitted through an authorised University account, which is necessary to provide an audit trail of user activity on the network.

2.2 Staff and students who are authorised to access resources through the University network should be inducted and be given the appropriate training to ensure that University network policies are known and are understood, and that guidance as set out in the Janet AUP is followed. Guidance relating to the way information is managed in the institution can be found in the Information Security Management System (ISMS) which can be found at:(http://www.glos.ac.uk/isms/responsibility.cfm) Any staff and students found in breach of these guidelines may be subject to University disciplinary procedures.

2.2 Any software must be approved by ICT Services prior to the installation on University computers, to help minimise the risk of virus infection that may have a damaging affect on the operation of University's systems.

2.3 It is an offence for users to misuse the University's computer systems and networks. Examples of such misuse include:

i. Accessing a University system or network without authority;

ii. Using a username/password that belongs to another student or member of staff;

iii. Using shared passwords;

iv. Failure to comply with security requirements as defined in the Universities Information Security Management System (ISMS) that contains guidance for users;

v. Sending e-mail to large groups of individuals when this has not been formally authorised;

vi. Accessing commercial or personal data when not authorised to do so or for a purpose otherwise than in connection with an individual's duties for/within the University;

vii. Installing and using non-approved software, which is software that has not been installed or approved by the LIS ICT Department;

viii. Installing and using non-licensed software;

ix. Installing and using non-approved hardware;

x. Unauthorised copying and distribution of electronic copyright material;

xi. Unauthorised commands or programs that have the potential to affect systems performance or accessibility;

3. E-Mail Policy

This policy governs the use of the University's e-mail system to facilitate the exchange of electronic information both internally and externally in the institution.

It is important to note that the University staff and student e-mail systems are key communications systems in the institution. Inappropriate use of the e-mail system can lead to virus infection, which ultimately could lead to a degradation of network performance, or in extreme circumstances take the whole of the University network down.

3.1 Computer Viruses

Incoming e-mails and their attachments may carry dangerous or potentially business damaging viruses. If an individual is in any doubt about the contents of an e-mail message and suspects the existence of a virus they should not open it, but must consult the ICT Helpdesk (4044) immediately to obtain technical assistance.

In relation to outgoing e-mails, staff or students may be held liable if e-mails containing *'harmful'* content such as computer viruses, are sent either internally or externally. If there is any doubt regarding e-mail attachments, the ICT Helpdesk should be contacted immediately on 4044.

3.2 Offensive or obscene e-mail

If there is any reason to suspect that an incoming e-mail may contain offensive or obscene material, where possible, refrain from opening it. Under no circumstances should the e-mail be sent on to another user, and it should either be reported to the ICT Helpdesk, or deleted immediately. Never send via e-mail pornographic or other any offensive materials that contravene University policy, the Janet AUP or UK legislation.

3.3 Confidentiality

E-mail communication is not always a secure means of communication across the internet. Consider the need to send strictly confidential, or commercially sensitive messages by the Internet without the prior consent of the intended recipient. Attachments containing sensitive information should be password protected or encrypted.

Personal e-mail messages may be open to scrutiny without an individual's permission. For example, ICT Services in the course of their duties may have to investigate the contents of e-mail which has been delivered to an unknown e-mail address

(Further information regarding the monitoring of communications in the University ca be found at: http://www2.glos.ac.uk/offload/departments/personnel/phbk/part13/13.22monitoringOfCommunicationsLegislativeFramework.pdf)

All outgoing e-mails should contain the sender's name, title and contact information using the standard university email signature block

3.4 Content

E-mails should not be treated as an informal means of communication. Always use professional language when e-mailing internally or externally. E-mail is accepted in law as evidence and therefore legislation relating to Data Protection and Intellectual Property applies equally to e-mail messages, so the same care should be given to the tone and content of e-mails as for paper communication.

3.5 Checking your e-mail

University mailboxes should be checked regularly and messages answered in a timely manner. If a user is going is not going to be in the University to respond to their e-mails for an extended period of time, then they should either;

- Authorise or delegate access to another staff member, who will check the e-mails so that important information is not missed.
- Arrange to access their email remotely via web mail.
- Set up an out of office rule to automatically forward and/or respond to mail (auto respond is not recommended if an individual regularly receives SPAM mail as it confirms to the sender that their mailbox is active and will attract more unwanted mail)

3.6 Printing e-mails

It is not good University practice to print out e-mails. However, from time to time it may be necessary to obtain a hard copy of appropriate e-mails to record an audit trail for relevant University business. Confidentiality of information stored should be in-line

with the guidelines set out in the Information Control policy at:http://www.glos.ac.uk/isms/responsibility.cfm

3.7 Unnecessary Messages

Do not create e-mail congestion by sending trivial messages, or unnecessary e-mail messages. Staff and students are required to ensure that:

- E-mails are not circulated through the University's " Allusers" facility, without the express consent of the appropriate authority; i.e. ICT manager - for students; Personnel & Staff Development - for staff.
- E-mails are kept as short and accurate as possible.
- Large attachments *(over 5Mb)* should not be sent unless there is no other reasonably practicable way of delivering the data .

3.8 Personal Use

The University allows the limited personal use of the e-mail system, provided that such personal use does not interfere with the main business activities of the institution, and does not jeopardise the effective operation of the University's systems and services.

3.9 Unauthorised Use

The University will not tolerate the misuse of the e-mail system. The following are examples that are considered a misuse of the system:-

i. Any message that could constitute bullying or harassment (e.g. on the grounds of sexuality, race, disability or age) or that could be considered offensive, obscene or in bad taste;

ii. Any message that could constitute defamation, for example in relation to other students, or members of staff within the University;

iii. Persistent unauthorised personal use, including but not limited to personal messages, social invitations, jokes, cartoons or chain letters;

iv. On line gambling;

v. Accessing, circulating, distributing or otherwise publishing pornography internally within the University or externally;

vi. Sending or distributing copyright information and/or any software available to the user;

vii. Posting confidential information about other students, staff members, the University or its suppliers;

viii. Sending of unsolicited e-mail to internal or external recipients;

3.10 E-Mail Etiquette *(See Appendix I)*

4. Internet Policy

The main aim of this policy is to provide advice and guidance to create a safe and secure environment for staff and students to undertake University business over the Internet.

All users of the network must abide by the terms and conditions as set out in the Janet AUP, which can be viewed in each Learning Centre or over the web at: http://www.ja.net/services/publications/policy.

Using the Internet for any illegal activity, including violation of copyright or other legal rights, the unauthorised transmission or receipt of proprietary information, or transmitting any material that is in breach of UK legislation, is not allowed. In addition, the Internet should not be used for the transmission of, retrieving, observing or storing of any communication that is:

i. Discriminatory or harassing in any sense whatsoever and whether prohibited by the law or not;

ii. Pornographic or derogatory to any individual or group;

iii. Involves accessing entertainment, sport or gambling websites or other websites which have no legitimate connection to the University's business;

iv. Defamatory or threatening, whether legally actionable or not;

v. Illegal or contrary to the University's policies or business interests;

The University operates proxy, filtering and firewall systems designed to provide a safe and secure environment, to assist the effective flow of electronic information, both in and out of the institution. Any user found wilfully trying to circumvent the security of network systems, will be subject to University disciplinary procedures.

Under 18 year olds may only access the Internet through University computers with the written consent of a parent or guardian, who must

take responsibility for the child by agreeing to abide by the University Internet & E-mail policy, and the Janet AUP.

A degree of filtering can be applied to all designated child accounts. However, it should be noted that whilst every effort will be made to block access to illegal and 'undesirable' sites, current filtering technology cannot block all offensive sites. Therefore, Learning & Information Services cannot guarantee that users will not accidentally access information and/or images that individuals may find offensive or disturbing.

4.1 Personal Use

The University allows the limited personal use of the Internet, provided that such personal access does not interfere with the main business activities of the institution, and does not jeopardise the effective operation of the University's systems and services.

4.2 Personal Privacy and Monitoring

The University assumes that its staff and students will act in a reasonable manner and adhere to the highest standards of conduct in the use of ICT Systems. The University maintains a full audit trail of activity but does not monitor day-to-day email or Internet activity under normal circumstances. However, the University reserves the right to monitor activity to ensure that the systems are being used for legitimate business purposes including the following:

- To ensure compliance from time to time with the University Email & Internet policy and the Janet Acceptable Use Policy (AUP)
- To prevent or detect the unauthorised disclosure of any information which is confidential to the University. For these purposes any information held within the University's Systems is to be treated as being confidential unless the University has taken active steps to publish the information. Confidential information includes details of the University's students, suppliers, employees, financial or trading results, and any details relating to the University's services.

The University reserves the right to monitor patterns of computer use, websites accessed, connection lengths and times at which connections are made. These may be monitored for legitimate purposes including:

- Cost analysis;

- Resource allocation;
- Optimum technical management of information resources;
- Detecting patterns of use that indicate students or staff members are violating University policies or engaging in unauthorised activities.

The University reserves the right at its discretion, to review the electronic files and messages of any user of the University-supported Internet connection.

4.3 Safeguarding Access to Workstations

Workstations should not be left unattended as this provides an opportunity for others to access the e-mail system and send items in your name. A password screensaver should be used to prevent unauthorised access.

All network users are issued with a unique username and password which is changed at regular intervals and is confidential to the user. However, it may be required at times for users to disclose their passwords to authorised ICT Services staff, to help ensure compliance with University policy and maintain the integrity of University computer systems.

(Supplementary information in the area of Information Security can be found at: http://www.glos.ac.uk/isms/responsibility.cfm)

Appendix I

E-Mail Etiquette

Electronic mail is a relatively new form of communication, and the number of new users is increasing dramatically. With more established forms of communication such as traditional post and telephone, certain widely-observed *conventions* are used. Such courtesies as when to use "yours sincerely" in a letter, or announcing your name and/or number when you answer the telephone, are not just pointless conventions, they help to promote a sound basis for communication between the relevant parties. Because e-mail is a relatively new form of communication, few people are aware of suitable or appropriate conventions to use.

These conventions (often called "network etiquette", or "netiquette") recognise that it is very easy to send emails very quickly, and so little thought may be given as to how the message will be received.

The following is a summarised list of *Do's* and *Don'ts* to help promote a code of good e-mail practice in the University.

Do's

i. Check your mail regularly
ii. Always reply, even if the reply is brief
iii. Try to reply promptly to avoid any confusion about whether an e-mail has been received
iv. Develop an orderly filing system for email messages you wish to keep, and delete unwanted ones to conserve the allocated 200Mb of server disk space
v. Try to keep email messages fairly brief, *(max. 2 screen fulls)*
vi. Try and make sure that the *"Subject"* field in email messages is meaningful, to help put the e-mail into context. Also, when the reply option is used, ensure that the subject field still accurately reflects the content of your message
vii. Try to restrict yourself to one subject per message, this helps recipients to use the "subject" field to manage their messages
viii. Be tolerant of others user's mistakes on e-mail. Some people are relatively new to this medium and may not be good typists
ix. Consider the tone and content of e-mail messages, particularly, at busy or stressful times

x. Remember that people other than the person to whom it's addressed may see your message; i.e. cc - distribution list
xi. Consider the circulation list for outgoing e-mails. i.e. is the e-mail you are sending appropriate to everyone on the distribution list?

Don'ts

i. Do not send e-mails in the *'heat of the moment'*. Reflect on the issue, and then send a considered response later
ii. Do not reproduce an email message in full when responding to it, especially if you are posting to a bulletin board. This is hard on the readers and wasteful of resources
iii. Do not extract and use text from someone else's message without acknowledgment, as it is plagiarism
iv. Do not make changes to someone else's message and pass it on without making it clear where you have made the changes
v. Don't pretend you are someone else when sending mail, e.g. by using someone else's account to send it.
vi. Do not broadcast email messages unnecessarily. e.g. do not send or forward chain email, as it can offend some people and again it is wasteful of network resources.
vii. Do not send abusive or defamatory messages. Apart from being discourteous and/or offensive, it is contrary to University policy and may break the law

In addition:

viii. Remember that sending email from a University account is similar to sending a letter on letter-headed paper, so it is advisable not to say anything that might bring discredit or embarrassment to the University
ix. Remember that government legislation relating to written communication applies equally to email messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination.
x. Do not print out emails unless it is necessary to obtain a hard copy for record purposes

(Supplementary information on the University Communications policy can be found at: http://www2.glos.ac.uk/offload/departments/personnel/phbk/part13/13.12communicationPolicyAndGuidelines.pdf)

2 Standards

2.1 Hardware

Desktop computers will be Personal Computer (PC) based, except where there is a good reason or an appropriate business case to use an alternative platform. All computers will be supplied by one of the recommended Southern Universities Purchasing Consortium (SUPC) suppliers to the University, and shall be purchased through the University's ICT Purchasing Manager.

Where possible, Apple Macs will continue to be phased out for administrative purposes, but will still be supported in academic areas where there is educational benefit.

To support the interchange of data between corporate information systems, where possible, network and application servers will also be PC based running the appropriate Microsoft operating system.

For security purposes, any computer purchased for office use must include a securing device as approved by Learning and Information Services, particularly computers located on the ground floor of premises. Security devices will be purchased at the same time as the new computer. Local arrangements should be made with Facilities Services regarding the fitting of these security devices.

All computers and associated devices such as printers, scanners, etc. used on the University network, should be registered on the University ICT inventory managed through the ICT Helpdesk.

2.2 Software

The principles that underpin the purchase of software are:

i. Sound academic or administrative rationale
ii. Compatibility and consistency of practice
iii. Value for money.

The University supports the purchase of University software site licences, particularly where Value for Money (VfM) can be demonstrated that will benefit the whole organisation. For example: The Microsoft Campus agreement scheme, enables the University to use the most recent version of a range of Microsoft Software at a substantial discount over normal prices.

The University has standardised on the Microsoft Office suite of applications to provide improved access to digital forms of information and assist in the seamless interchange of electronic data. The Academic Development Unit (ADU) provides training and support for a range of software applications that include the Microsoft suite of applications. Further details of software training can be found at: https://ict-training.glos.ac.uk/elearning/

Whilst the Department of Learning and Information Services are responsible for the maintenance and support of generic Microsoft software applications in the University, testing and support of specialist software remains the responsibility of the relevant Campus, Faculty or Department.

When the University has the opportunity to replace systems software through the annual ICT capital programme, software applications should be based on web enabling technologies that will assist in the development of a University-wide Managed Learning Environment (MLE). The MLE aims to provide simplified access to electronic forms of data through customised information portals, for both staff and students.

Heads of Schools/Research Units and Heads of Departments are responsible for software installed on computers located in their area of responsibility, and are required to provide an annual return to update the University ICT inventory.

Learning and Information Services are responsible for the student computing network and the delivery of software applications through a customised desktop personalised to the needs of the individual. Testing and evaluation of new software applications should be undertaken in collaboration and partnership with ICT Services to ensure that software works successfully on University computers. A minimum of between 4 - 6 weeks should be allowed to enable a thorough evaluation and testing of any new software applications.

UNIVERSITY OF GLOUCESTERSHIRE

UNIVERSITY PHONE POLICY

1.0 Introduction

The University telephone system is managed by Learning & Information Services that delivers a service to both staff and students. Student calls in halls of residence locations are made through Calling Cards which can be purchased through reception areas and Learning Centres.

Each staff telephone is allocated to a cost centre, and call charges are paid for by the relevant Campus, faculty or Department through quarterly charges administered by Learning & Information Services. Maintenance and leased line costs are managed and funded centrally through Learning & Information Services.

2.0 Mobile Phones

Mobile phone services are managed and coordinated by Learning & Information Services through a centralised agreement with Vodafone. Requests for mobile phone services should be approved through Campus Deans/HoD, and then forwarded to the University ICT Manager for action.

3.0 Monitoring of University Phones

University of Gloucestershire reserves the right to monitor the destination, volume and duration of all incoming and outgoing calls to University phones in support of the business interests of the University and to investigate complaints. Staff should be aware that their voicemail messages may need to be checked if they are absent, particularly if the absence is unexpected. Written approval for access must be given by a member of the Senior Management Team before any action takes place.

UNIVERSITY OF GLOUCESTERSHIRE

UNIVERSITY INFORMATION SYSTEMS POLICY

1.0 Introduction

The Information Systems Policy forms part of a framework of policies that support the use and development of Information, and Information and Communications Technology (ICT) systems in the University. In an increasingly information based society the development and effective use of ICT systems will become increasingly important. The University aims to have Information Systems that provide accurate and timely information, through a secure and easy to use interface, but retain the flexibility to meet the planning needs of the University. All key corporate information systems will be subject to systematic review over an agreed period of time as agreed by the Information Strategy Committee (ISC).

1.1 Purpose

The purpose of the Information Systems Policy is to provide guidance to support the procurement and development of information systems in the University. It is the intention, through the use of information and communications technology, to reduce costs, enhance services, and provide management information to support development of the learning, teaching, research, administration, and management processes of the institution. All new systems will be reviewed against the principles as laid out in the University's Information Strategy and will be purchased within the framework of developing a Managed Learning Environment (MLE), to help achieve a joined-up and integrated approach to systems development. New systems should be Lightweight Directory Access Protocol (LDAP) compliant, and where possible, accessible through a web enabled interface.

1.2 Current position

(a) **Support for administrative systems**

Support for Corporate Information Systems (CIS) is split between two University departments. Finance & Planning assume responsibility for the development of key information systems such as SITS, HRS, Finance, etc., and Learning & Information Services (LIS) assume responsibility for the hardware and software, and ensuring that the hardware has a high availability on the network. External consultants, and software suppliers are used to provide a 'high-level' of systems expertise that cannot be provided through 'in-house' technical support.

(b) **Information sharing**

To assist in the effective sharing of information and the transfer of data between users and systems, Information systems need to comply with the nine key principles as laid out in the University's Information Strategy.

(c) **Staff Development and Training**

Short-term systems training to solve identified skill gaps will be provided through discussion with Finance & Planning, ICT Training unit and Learning and Information Services. In the medium to long term corporate data will be made available through web interfaces on the University Intranet, obviating the need for specific systems training.

(d) **Current Systems**

Corporate information systems have been developed in partnership with external suppliers and user departments to satisfy user requirements. Each system will be reviewed on a regular basis, and as a guide an outline 5 year review programme is provided in 2.3

1.3 **Management Information Systems Development**

Key parameters for the development of MIS in the University are that:

a) systems will be purchased with the primary aim of meeting the business needs of the institution;

b) systems' selection will be based on the expertise and business knowledge of the system and data owners;

c) technical expertise will be provided by LIS;

d) small, specific, individual, and cost-effective software packages will be used to satisfy changing internal and external information needs;

e) the University will use networked desktop machines and thin client technology to integrate systems, and provide for the sharing and transfer of electronic data;

f) report writing and the ability to manipulate data, which can be analysed and synthesised to inform decision-making, will be important considerations when new systems are to be purchased

2.0 Systems Development and Replacement

2.1 **Procedures**

(a) Corporate Information Systems will be regularly reviewed through the University's Information Strategy Committee (ISC). Reviews of individual systems will be undertaken by a small working group as agreed by Chair of ISC, with representation from F&P, LIS and a cross section of system users. The working group will normally undertake an information audit, and produce a needs analysis reflecting the changing business and information needs of the University and its customers in relation to the system under review.

(b) The resulting report will be considered by the ISC to establish whether system upgrading or system replacement is the most appropriate way forward, together with outline costs to assist decision making.

(c) Where system replacement is most appropriate, the project team will prepare an Invitation to Tender (ITT), and a minimum of three tenders will be sought. The tender process must include an opportunity for system users to evaluate the systems under consideration and to express their opinion on each system.

2.2 **Considerations**

System selection will be guided by the parameters stated in section 1.3, and other factors of specific relevance to the system under review. Factors of particular importance are currently:

(a) **System Integration and Report Writing**
Report writing facilities and system output for both internal and external users of the system, and integration with other University systems, are important selection criteria, which must be considered during the system replacement process.

(b) **Management Information Systems**
The interface between Management Information Systems and its main users will be clearly defined through Service Level Agreements (SLAs). SLAs will be developed in collaboration and consultation with user departments, and will be monitored and reviewed on an annual basis by ISC. System upgrading and procurement present ideal opportunities to define and refine Service Level Agreements

(c) **Devolved access to data**
Staff access to corporate information systems such as Student Records, Finance and Human Resources System can only be provided through prior agreement with the System Owner of

the relevant system. Where possible, authorised access will be provided through a web enabled interface consistent with University Information Portal developments

(d) **External Links**
System review project teams should make use of information provided by external agencies and organisations, such as the UCISA, JISC, SCONUL, etc., who represent the current views of the HE sector.

(e) **Supplier information**
System review project teams should ensure that suppliers can continue to support the University post-purchase by scrutiny of supplier financial reports, use of reference sites, and other third party information. System purchase should normally incorporate negotiation of an ESCROW agreement.

2.3 **MIS review and draft replacement schedule**

2007/08	2008/09	2009/10	2010/11	2011/12
Complete implementation of Finance System Develop new Internet Server in Sharepoint	Review Timetabling System Develop customised Information Portals in Sharepoint	Review Human Resources System	Review SITS	Review Library Management System