Policy Number	**: POL-ICT-08-01**
Title	**: Information and Communication Technology Use Policy and Procedure**
Effective Date	**: 15 March 2008**
Category (Top & 2ⁿᵈ level of CCV)	**: Information Management, Systems**
Organisational Unit	**: ICT Department**

1. POLICY PURPOSE

The University will establish policy, standards, guidelines and procedures to ensure that Information, Communication and Technology facilities, services, programs and data are protected from all threats, whether internal or external, deliberate or accidental.

2. APPLICATION

This policy applies to any Curtin or User owned facility connected to the Curtin campus network and is covered by this policy and related policy's.

3. EXCEPTIONS

3.1 The University electronic messaging services or email may be used to send or receive incidental personal messages providing that such use will not:
Directly or indirectly interfere with the University business operations, or
Interfere with the user's employment or other obligations to the University, or
Cause or be likely to cause damage to the University's reputation, or
Conflict with any University policies, regulations or Malaysian Laws.

3.2 Any breach of this policy or associated ICT policy will be managed in accordance with the ICT breach policy. Disciplinary measures (as contained in relevant University statues and/or employer-staff agreements) apply, for violations of this policy and policies associated with this policy.

4. DEFINITIONS

The following definitions apply to all sections of this manual.

4.1 Appropriate and responsible manner means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University. Use must also be consistent with the specific objectives of the project or task for which such use was authorized. Any use inconsistent with these objectives is considered to be inappropriate use and action may be taken under the University ICT Information Security Incidents and Breach Policy.

4.2 Breach means an information security incident that involves users not using Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner.

4.3 Copyrighted content means material for which the copyright for the content is held by a third-party other than Curtin University of Technology. E.g music, computer software, films and video.

4.4 Electronic Messaging Services means information technologies used to create, send, forward, receive, store, or print electronic messages.

4.5 Electronic Identity means the set of essential information about an individual that is stored electronically by the University.

4.6 Electronic Identifier means the value that is used in Curtin electronic systems to uniquely identify an individual. An electronic identifier is an attribute of the electronic identity.

4.7 Information and Communication Technology facilities and services mean any information resources provided by the University to assist or support teaching, learning, research and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study or research, all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, personal digital assistants, electronic email systems, internet, intranet and extranet.

4.8 ICT facilities and services covers:
   a) All types of ICT facilities owned or leased by the University and ICT services provided by the University
   b) Computer equipment owned or leased by Users, which are used to connect to the University networks and/or the Internet

4.9 Information security incident means any information security event that disrupts the expected standard operation of ICT services and facilities.

4.10 Infrastructure means the physical equipment used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, and also the router, aggregator, repeater, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals and data that are transmitted.

4.11 Objectionable material as defined by the Malaysian Censorship Act 2002, including material such as child pornography, incitement to violence, torture, and bestiality.

4.12 Operating System(s) means the main control program that runs a computer and sets the standard for running application programs. It is the first program loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programs and errors, and directing input and output.

4.13 P2P Application is software running on device to provide the communications of file sharing capabilities between peers. This software is usually downloaded from the Internet and includes but not limited to applications such as Kaaza, BitTorrent, Peercasting and Limewire.

4.14 Record means any record of information however recorded and includes:
   a) Anything on which there is writing or Braille
   b) A map, plan, diagram or graph
   c) A drawing, pictorial or graphic work or photograph

c)   Anything on which there are figures, marks, perforations, or symbols, having a meaning for persons qualified to interpret them

d)   Anything from which images, sounds or writings can be reproduced with or without the aid of anything else and

e)   Anything with information has been stored or recorded, either mechanically, magnetically or electronically.

4.15 Restricted material as defined by the Malaysian Censorship Act 2002, including any material that a reasonable adult, by reason of the nature of the material, or the nature or extent of references in the material, to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear.

4.16 Software a specific use for a computer program, such as for accounts payable or payroll. The term is commonly used in place of the terms "application", "operating system" or "program." Examples of programs and software include pre-packaged productivity software (such as spreadsheets and word processors) and larger, customized packages designed for multiple users (such as e-mail).

4.17 Staff member means any person who has been offered and has accepted a contract of employment with Curtin University of Technology.

4.18 Student means a person who is admitted to, or enrolled in, a unit, course or program of study approved by Curtin University of Technology, which leads to, or is capable of leading to, an academic award of the University. For the purposes of this definition, the academic awards of the University are as recorded in the List of Academic Awards of Curtin University of Technology.

4.19 Use of Electronic Messaging Services means to create, send, forward, reply, copy, store, print, or possess electronic messages. For the purpose of this procedure, receipt of an electronic message is excluded from this definition to the extent that the recipient may not have control over the content of the message received.

4.21 User means a staff member or Students of Curtin University of Technology, Miri Campus.

4.22 Virus means malware software such as computer viruses, worms, trojan horse and spyware programs.

5. **POLICY USE STATEMENT**

5.1. The University shall issue a unique username and password to staff, students and University Associates to enable the appropriate and responsible use of ICT facilities and services.

5.2. All users who are granted access to or use University Information and Communication Technology facilities or services shall use these facilities and services in an appropriate and responsible manner.

5.3. The university reserves the right to record and monitor activity, limit, restrict, cease, or extend access of ICT facilities and services.

5.4. Disciplinary actions apply, for violation of this policy and/or procedures.

5.5. Any breach of this policy or associated ICT policy will be managed in accordance with the ICT breach policy. Disciplinary measures (as contained in relevant University statues and/or

employer-staff agreements) apply, for violations of this policy and policies associated with this policy.

    5.5.1.Objectives

        a)   To ensure that ICT facilities and services are used in an appropriate and responsible manner.

        b)   To safeguard the integrity and security of the ICT facilities and services.

6. OBJECTIVES or PRINCIPLES

6.1. To minimize University asset and business risk.

6.2. To ensure that all of the University computing facilities and services, programs and data are adequately protected against loss, misuse or abuse;

6.3. To create a University awareness that appropriate information and physical security measures are implemented as part of the effective operation and support of ICT facilities and services;

6.4. To ensure that all users fully comply with Information Security policy, standards, guidelines and procedures, and the relevant Malaysian legislation;

6.5. To ensure all users are aware of their responsibilities for the security and protection of facilities, services, programs and data over which they have control.

6.6. To ensure that the information security aspects of technology and business applications are consistent with the University Information Security Architecture;

6.7. To where practicable apply the principles of Information Security standard ISO 17799;

7. STUDENT Electronic Messaging Policy (eMAIL)

All students accessing and using the Student Electronic Messaging Service shall comply with this procedure.

7.1. OBJECTIVE(S)

7.1.1 To ensure consistent understanding of student responsibilities when using the Student Electronic Messaging Service.

7.1.2 To identify administrative, support and maintenance requirements for the Student Electronic Messaging Service.

8. ADMINISTRATIVE PROCEDURES

8.1. Access to the Student Electronic Messaging Service

A student's electronic identifier and password is used to access SEMS via Student Webmail. Students will be issued with an electronic identifier and password in accordance with the Student Login Procedures.

8.2. Activation of Student Electronic Messaging Service Accounts

Students will automatically be granted access to SEMS on admission to the University.

8.3. De-activation of Student Electronic Messaging Service Accounts

A student's access to their SEMS account will be de-activated if:

    a)   use is deemed inappropriate; or

    b)   they have been terminated or have withdrawn from their course of study; or

    c)   3 months have passed since they have completed their course of study; or

d) they have been classified as 'absent without leave' by discontinuing their course of study without formally notifying the University, and

e) they have not been admitted to another course of study.

8.4. **Re-activation of Student SEMS Accounts**

The University will re-instate access to SEMS for students who have been admitted to a new course or who re-enrol after access has been de-activated.

8.5. **STUDENT RESPONSIBILITIES**

8.5.1. **Limitation on Message and Attachment Size**

a) Students shall attempt to minimise network traffic by reducing the size of large messages and attachments prior to transmission. Attached files should be compressed to minimise network traffic.

b) Electronic documents in excess of Curtin's current maximum allowable size may automatically be excluded from transmission by the network server gateway restricting mechanism.

8.5.2. **Professional and Ethical Use of Messaging Services**

a) In general students cannot be protected from receiving offensive electronic messages. Students using SEMS shall act in a professional and ethical manner. In order for this to be achieved the following conditions apply:

b) Students shall apply the same personal and professional courtesies and considerations in electronic messages as they would in other forms of communication.

c) Students shall not transmit messages unnecessarily.

d) Students shall not transmit frivolous, abusive or defamatory messages.

e) Students shall not harm minors through messages.

f) Students shall not transmit electronic messages that are illegal or contravene other University policies.

g) Students shall express themselves carefully in order to clearly convey their message and not create any uncertainty in the mind of the recipient about the contents of the message.

h) Students shall not disguise the content of the original message.

i) Students shall not make available any content that they do not have rights to.

j) Students shall not cause interference with other users of electronic mail services. Examples of interfering techniques include transmission of e-mail chain letters, widespread distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same e-mail message.

k) Students shall not give the impression that they are representing, giving opinion or making statements on behalf of the University.

8.5.3. **Commercial for profit activities or advertisements**

a) SEMS may not be used for commercial activities or personal gain, except as permitted by other University policies.

9. Advertising or sponsorship is not permitted except where such advertising or sponsorship has been approved by the University.

9.1.1. **Message Storage**

In accepting access to SEMS, students consent to their electronic messages being stored both on-line and off-line (as a consequence of routine system backup operations).

9.1.2. **Non-compliance**

Students who contravene this procedure may be subject to the provisions of the ICT Breach Policy.

9.2. **SUPPORT AND MAINTENANCE PROCEDURES**
9.2.1. **System Accountability**
Under no circumstances is the University accountable for loss of electronic messages.

9.2.2. **Duties of the Student Messaging Administrator**

The physical and logical security of electronic messaging services (records, data, application programs, and system programs, etc.) is the responsibility of ICT Department. On occasion such personnel might, during the performance of their duties, inadvertently see the contents of electronic messages. Except as provided elsewhere in this procedure, such personnel are not permitted to do so intentionally or to disclose or otherwise make use of what they have seen. The exception is that of systems personnel who may need to inspect the message content in order to perform their duties.

9.2.3. **Inspection and Monitoring of Electronic Messages**
a) **Privacy**
   i) Due to the nature of electronic messaging systems, the University cannot guarantee the confidentiality of information.

   Ii) Students should also note that system logs might contain the sender and originator addresses of both incoming and outgoing electronic mail messages.

   Iii) The University respects the privacy of users. It does not intend to routinely inspect or monitor electronic messages. However, viewing of stored messages may be necessary from time to time to satisfy the requirements of the Freedom of Information Act 1992, to help redirect messages that cannot be delivered, to examine contents for legal reasons, or for other operational purposes such as messages that cause failures in the system due to the presence of viruses, size, or message corruption.

1. Consent and Compliance

The student's consent will normally be sought by the University prior to any inspection, monitoring or disclosure of University electronic messaging records in the University's possession.

2. Inspection of Electronic Messages without Consent

8.6.4 The University permits the inspection, monitoring or disclosure of electronic messages without the owner's consent only when:

    a) consistent with, and required by law;

    b) there is substantiated reason to believe that violations of law or University policy have taken place; or

    c) in exceptional cases, to meet time-dependent, critical operational needs.

When access to an individual's electronic message is required and is consistent with one of the above items, one of the following may apply:

(a) Authorisation

Except in emergency situations, such actions must be authorised in advance and in writing by the authority specified by the law or policy under which the action is taken. If the authority is not specified, authorisation must be sought from the appropriate Dean, Divisional Head, Departmental Manager on the advice of the ICT Manager. The advice of the University's Director, Legal Services should normally also be sought prior to authorisation because of changing interpretations by the courts of laws affecting the privacy of electronic messaging. At the earliest possible opportunity, the University shall notify the affected individual of the action taken and the reasons for the action taken, unless law or other University policy specifically requires otherwise.

(b) Emergencies

In emergency situations (e.g. when the community or its members are endangered or to maintain the integrity of information and services when access to electronic messaging services must be secured to ensure the preservation of evidence) special dispensations apply. The ICT Manager, the appropriate Dean, Divisional Manager, or Head of Faculty/Department/Area may immediately take whatever is the minimum necessary action to resolve the emergency. This may be done without authorisation with respect to the services under their respective control, but appropriate authorisation must be sought immediately following the procedures described above. If the action taken is not subsequently authorised, the ICT Manager will seek to have the situation restored as closely as possible to that which existed before action was taken.

8.7 Accountability

8.7.1 Responsibility for compliance with this procedure

    a) Students are responsible for reading and complying with this procedure and any associated policies, procedures, guidelines or conditions of use.

    b) By logging on to the Student Domain, students accept this procedure and any published policies, procedures and conditions of use that apply to SEMS and electronic facilities and services provided by the University.

8.8 ICT breach Policy

Any alleged breach of the Curtin's ICT Acceptable Use Policy, in Miri Campus, shall be reported to ICT Department who will record, investigate and act accordingly to this policy.

8.8.1 OBJECTIVE(S)

To ensure consistent and expedient investigation and management of alleged breaches.

8.8.2 MANAGEMENT OF BREACHES

a) Breach Reporting

Any reported information security incident that is considered to be an alleged breach of ICT policy or procedures will be categorised into:

- i) Minor breach - as defined in Schedules A and B.
- ii) Major breach - as defined in Schedules A and B.

All breaches are investigated to determine whether a breach was of an accidental or deliberate nature.

Consistent categorisation of breaches and recommended disciplinary actions across the University apply. Guides to the applicable response are described in the following Schedules:

- i) Breaches by Staff: Schedule A.
- ii) Breaches by Students: Schedule B.
- iii) Example categorisation of breaches: Schedule C.

b) Breach Management Reporting

- i) Quarterly management summary reports of breaches are published.
- Ii) Priorities will be assigned to breaches based on the severity of the impact on the University.
- Iii) Confidentiality of information related to individual users is maintained at all times.

8.3.3 BREACH PENALTIES

a) INTERNET BREACH

Depending on the type and circumstances of an Internet use breach the following external access restriction penalties will apply:

- i) Password/Account - 20 days
- ii) Pornography   - 14 days
- iii) Copyrighted Content - 14 days
- iv) All other - 7 days (after first warning)

Pornography and Copyrighted Content repeat breaches will incur a 20 day external Internet limited access restriction and will be subject to ICT Breach Policy action.

As necessary University network or external Internet access may be suspended.

Depending on the breach history subsequent breaches may result in external Internet access being fully restricted and escalation to the Divisional Administrator or Head of Department for disciplinary action.

Recovery of unnecessary Internet traffic costs will be considered and actioned where appropriate.

b)   **SCHEDULE A – CATEGORIES OF BREACH FOR STAFF**

Minor Breach

Any activity jointly considered by the staff member's Manager or nominee and the ICT Manager as inconsistent with the staff member's responsibilities	Email warning & recipient acknowledgement Interview optional	Optional notification to Divisional Administrator or Head of Department Staff disciplinary procedure

Major Breach

Any audio- visual copyright breach e.g. music, films, videos	Staff disciplinary procedure
Use of copyright software outside the University's License provisions	Staff disciplinary procedure
Giving access to Restricted material to a minor/s	Staff disciplinary procedure Anti Corruption Commission or Police to be advised
Viewing, downloading, storing, sending or giving access to Objectionable material	Staff disciplinary procedure Anti Corruption Commission or Police to be advised

c)   **Schedule B – CATEGORIES OF BREACH FOR STUDENTS**

Minor Breach

Any activity jointly considered by the student's Head of Department or nominee and the ICT Manager as inappropriate and irrelevant to the student's academic progress	Email warning & recipient acknowledgement Interview optional	Optional notification to Divisional Administrator Student disciplinary procedure

Major Breach

Any audio- visual copyright breach e.g. music, films, videos	Student disciplinary procedure
Use of copyright software outside the University's License provisions	Student disciplinary procedure
Giving access to Restricted material to a minor/s	Student disciplinary procedure Police to be advised
Viewing, downloading, storing, sending or giving access to Objectionable material	Student disciplinary procedure Police to be advised

NOTE:
Any information security incident where a legal infringement is suspected MUST be dealt with as a major breach.

Schedule C provides a guideline on breach types and breach categories.

d)   SCHEDULE C - EXAMPLE CATEGORISATION OF BREACHES

Doing anything dishonest or illegal. E.g. plagiarising an assignment (i.e. presenting someone else's work as your own).	Major

Copying or sharing with others software, music or movies without the written permission of the copyright owner. Some examples:
   Copying or sharing sound recordings, films, videos, radio and television broadcasts via email, CD or other electronic means.
   Making a CD track or movie available via a file-sharing service (e.g. Napster, Kazaa, or other peer-to-peer services), an FTP service, or a web-site.
   Copying a videotape, CD, or DVD onto another videotape, CD, DVD, computer hard disk, or any other storage media.
   "Ripping" a music track to a Curtin disk or duplicating a music CD.
   Copying a computer file containing music or video onto a videotape, CD, DVD, computer hard disk, or any other storage media.
   Downloading a CD track or movie from a file-sharing service, a peer-to-peer service, an FTP service, or a web-site.
   Storing a file on University equipment that contains illegally copied software, music or video storing of files on a personal piece of equipment, copyrighted software or audio-visual material accessed using the Universities Internet service.
	Major

Hacking into, meddling with, or damaging any other computer or service. E.g. trying to "break into" or "crash" another computer on the Internet.	Major
Using another person's identity or authorisation codes. e.g., using someone else's username or password.	Major
Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based. e.g. "packet sniffers" and "password crackers".	Major

Viewing, downloading, storing, sending, or giving access to material deemed as objectionable by the Malaysian Censorship Act 2002. E.g. materials such as child pornography, incitement to violence, torture, and bestiality.	Major
Giving a person under the age of eighteen years access to material regarded as restricted by the Malaysian Censorship Act 2002. E.g. materials involving sex, drug misuse or addiction, crime, cruelty, and violence.	Major
Harassing any person. E.g. sending obscene messages, language, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.	Major
Unauthorised use of access accounts and/or passwords	Major
Theft of any ICT Curtin hardware and software	Major
Unauthorised viewing, downloading, storing, sending, distributing or giving access to Restricted material using Curtin facilities and services e.g. CD-ROM, USB thumb drive etc	Minor
Unauthorised use of peer-to-peer software	Minor
Obstruct other student's from using computers in a Curtin student computer laboratory. E.g. by using it for anything other than academic and research activities.	Minor
The use of Curtin facilities and services for the playing of games or chat sessions not associated with the teaching, learning, research or administrative functions of the University.	Minor

ICT breaches are not necessarily limited to those outlined above.

8.9 ICT VIRUS POLICY
The University will ensure that approved and maintained licensed anti-virus software from known and trusted sources is deployed, where appropriate anti-virus is available, on Information and Communication Technology (ICT) facilities owned or leased by the University and ICT services provided by the University in Miri Campus.

Disciplinary actions apply, for violation of this policy and/or procedures.

8.9.1 OBJECTIVE(S)
a)   To minimise the risk of virus infections to University ICT facilities and services.
b)   To ensure the integrity of University ICT facilities and services.

8.9.2 VIRUS MANAGEMENT
The University will:
a)   Employ virus management measures at appropriate points of the University network.
b)   Implement virus control software and procedures to ensure that all networked computer servers and ICT managed workstations are protected against virus infection.
c)   Immediately disconnect compromised ICT facilities and services from the University network and these will remain disconnected until the infection has been remedied.
d)   Manage mass virus infections/threats through the ICT emergency management process.

e) Not connect to the University network computer equipment owned or leased by users, without appropriate and maintained anti-virus software

f) Disconnect from the University network any user owned or leased equipment that does not have appropriate and maintained anti-virus software installed.

9.0 ICT PASSWORD POLICY

All University Information and Communication Technology (ICT) facilities and services that are provided by the University shall comply with the minimum standard for passwords contained within this policy.

Information and Communication Technology (ICT) facilities and services used to support and manage infrastructure are excluded from this policy.

9.1 OBJECTIVE(S)

To ensure that appropriate password controls are implemented that address the risk of unauthorised access into the variety of Information and Communication Technology (ICT) facilities and services at the University.

To establish a minimum set of password management controls which apply across Information and Communication Technology (ICT) facilities and services at the University as a baseline requirement.

9.2 MINIMUM STANDARD FOR PASSWORD
The minimum standard for password setting and change is:

Length of password	6 characters
Number of unsuccessful login attempts before the username is made inaccessible automatically (locked)	5 times
Duration of lockout period	60 minutes
Period after which a password must be changed	30 days (every 1 months) - Users have the ability to change their own passwords at any time
Reusability of old passwords	Users will not be allowed to use a password they have used before within the last 5 months

9.2.1 PASSWORD MANAGEMENT PRINCIPLES

All Business Owners shall ensure that controlled ICT services comply with the following password management principles.

a) Use a minimum of eight characters for a password.
b) Use at least one alphabetic and at least one non-alphabetic character in their password.
c) Have facilities to control the number of failed accesses.
d) Have time limits for their use.
e) Have management of the reuse of the same password.
f) Can be turned off on cessation or transfer of users.
g) Have a secure process for the transmission of new or replacement passwords
h) Ensure that all passwords used in automated and/or unattended processes are encrypted where possible.
i) When purchasing new Information and Communication Technology (ICT) facilities and services check whether the items comply with the minimum standards defined in this policy and report any areas of non-compliance to Information and Communication Technology manager.

Users issued with a password have a responsibility to change it immediately after he/she:

a) Has been issued with the initial default password.
b) Has used the same password for more than six months.
c) Is advised by Information Management Services – Information Security or their local ICT Support staff to change it.
d) Has reason to suspect the password has been observed or compromised.

Users must not:

a) Share the password with anyone.
b) Write the password down in an insecure location.

A breach of this policy will incur disciplinary action by the University.

9.3 TELECOMMUNICATION POLICY
9.3.1 Objective(s)
To outline policies relating to the use of telecommunication services in the University.

9.3.2 University Internal Directory Listing
The University reserves the right to publish extension listing details both in hardcopy format and electronically. This information will contain at least the person's first name, last name, extension number, title and the Faculty or Department as appropriate.

9.4 PEER-TO-PEER (P2P) POLICY
9.4.1 Objective(s)

Use of P2P applications for file sharing and entertainment is deemed to be inappropriate use and will not be permitted.

P2P usage enable sharing and distribution of copyrighted works, and the Copyright Act makes it illegal to make or distribute copyright materials without proper authorization from the copyright owner.

The university will enforce protocol or port level restrictions to prevent P2P activities.

Any breach of this policy or associated ICT policy will be managed in accordance with the ICT breach policy.

10 PROCEDURES

These are the procedures that related to administrative, responsibilities, support and maintenance, prohibited activities and accountability procedures.

10.2 ADMINISTRATIVE PROCEDURES

10.2.1 Termination of Employment
When a staff member's employment with the University ceases for any reason, the University shall deny access by the former staff member to their electronic messaging account.

10.2.2 Withdrawal of Access
A staff member's electronic messaging services shall be withdrawn, by the appropriate system administrator, when instructed by the ICT Manager, the Dean, Deputy Vice-Chancellor, Head of Faculty or Department Managers.

10.3 RESPONSIBILITIES
10.3.1 Professional and Ethical Use of Messaging Services

In general staff members cannot be protected from receiving offensive electronic messages. Staff members using the University's electronic messaging services shall act in a professional and ethical manner. In order for this to be achieved the following conditions apply:
   a) Shall apply the same personal and professional courtesies and considerations in electronic messages as they would in other forms of communication.
   b) Shall not transmit messages unnecessarily.
   c) Shall not transmit frivolous, abusive or defamatory messages.
   d) Shall not transmit electronic messages that are illegal or contravene other University policies.
   e) Shall not disguise the content of the original message.
   f) Shall not make available any content that they do not have rights to.
   g) Shall not cause interference with other users of electronic messaging services. Examples of interference include transmission of e-mail chain letters, widespread

distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same message.

h) Shall not give the impression that they are representing, giving opinion or making statements on behalf of the University.

10.3.2 Personal Use

The University electronic messaging services may be used to send or receive incidental personal messages providing that such use will not:

a) Directly or indirectly interfere with the University business operations, or
b) Interfere with the user's employment or other obligations to the University, or
c) Cause or be likely to cause damage to the University's reputation, or
d) Conflict with any University policies, regulations or Malaysian Laws.

The use of 'free' or 'non-university' suppliers of electronic mail services to convey university related business content is prohibited. Staff should be aware that University intellectual property rights may be compromised by the proprietary usage conditions of such providers.

10.3.3 Commercial for profit activities or advertisements

a) The University's electronic messaging services may not be used for commercial activities or personal gain, except as permitted by other University policies.

b) Advertising or sponsorship is not permitted except where such advertising or sponsorship has been approved by the University.

10.3.4 University Property

a) All electronic messages stored on University computing and networking facilities are deemed to be University records and may be subject to disclosure.

b) All electronic messages which are in support of University business is considered to be a University record, irrespective of the location or ownership of the facilities used to create or store the electronic record. Users of electronic messaging services must be aware of their responsibilities in regard to the management retention and disposal of University records (refer University Records Management procedure).

10.3.5 Message Storage

In accepting access to the University's electronic messaging services, staff members and University Associates consent to their electronic messages being stored both on-line and off-line.

10.3.6 Non-compliance

Non-compliance of this procedure may be subject to the provisions of the ICT Breach Procedure.

10.4 SUPPORT AND MAINTENANCE PROCEDURES

10.4.1 System Accountability

Under no circumstances is the University accountable for loss of electronic messages.

10.4.2 Inspection and Monitoring of Electronic Messages

It is not the policy of University to regularly monitor the content of electronic messages. However, they may be monitored from time to time to support operational, maintenance, auditing, security and investigate activities. Users should construct their communications in recognition of this fact.

Controllers will not monitor individual communications out of personal curiosity or at the request of individuals who have not obtained the prior approval of the Manager, Information and Communication Technology. However, it may be necessary for controllers to review the content of an individual user's communications during the course of a problem resolution.

10.4.3 Privacy

Due to the nature of electronic messaging systems, the University cannot guarantee the confidentiality of information contained in messages.

System logs might record sender and recipient addresses associated with both incoming and outgoing electronic messages.

The University respects the privacy of users. It does not intend to routinely inspect or monitor electronic messages. However, viewing of stored messages may be necessary from time to time to satisfy the requirements of the Freedom of Information Act 1992, to help redirect messages that cannot be delivered, to examine contents for legal reasons, or for other operational purposes such as messages that cause failures in the system due to the presence of viruses, size, or message corruption.

While the university respect the rights of its electronic communications users, including their reasonable expectation of privacy, it is also responsible for servicing and protecting its communication networks. To accomplish this, it is sometimes necessary to intercept or disclose, or assist in intercepting or disclosing communications.

a) Consent and Compliance
Consent will normally be sought by the University prior to any inspection, monitoring or disclosure of University electronic messages in the University's possession.

b) *Inspection of Electronic Messages without Consent*

The University permits the inspection, monitoring or disclosure of electronic messages without the owner's consent only when:

i)   consistent with, and required by law;

ii) there is substantiated reason to believe that violations of law or University policy have taken place; or

iii) in exceptional cases, to meet time-dependent, critical operational needs, or

iv) It is necessary to protect the university communication networks.

When access to an individual's electronic message is required and is consistent with one of the above items, one of the following may apply:

(a) **Authorisation**

Except in emergency situations, such actions must be authorised in advance and in writing by the authority specified by the law or policy under which the action is taken. If the authority is not specified, authorisation must be sought from the appropriate Executive Dean, Divisional Head, Departmental Manager on the advice of the ICT Manager. The advice of the University's Director, Legal Services should normally also be sought prior to authorisation because of changing interpretations by the courts of laws affecting the privacy of electronic messaging. At the earliest possible opportunity, the University shall notify the affected individual of the action taken and the reasons for the action taken, unless law or other University policy specifically requires otherwise.

(b) **Emergencies**

In emergency situations (e.g. when the community or its members are endangered or to maintain the integrity of information and services when access to electronic messaging services must be secured to ensure the preservation of evidence) special dispensations apply. The ICT Manager, the Dean, Divisional Head, or Head of School/Department/Area may immediately take whatever is the minimum necessary action to resolve the emergency. This may be done without authorisation with respect to the services under their respective control, but appropriate authorisation must be sought immediately following the procedures described above. If the action taken is not subsequently authorised, the ICT Manager will seek to have the situation restored as closely as possible to that which existed before action was taken.

10.5   PROHIBITED ACTIVITIES

The University's Email systems must not be used to:

a) Create or distribute chain letters, "junk" or "SPAM" mail

b) Send anonymous Email, or forge email messages to make them appear to come from another person

c) Disrupt another person's activities or reasonable use

d) Harass another person or send unwanted offensive material

e) Pass off one's own views as representing those of the University
f) Read, delete, copy modify email under the control of other users without authorization
g) Pursue commercial activities or personal profit, unless users are explicitly authorized by the University
h) Intentionally introduce, distribute, propagate or create viruses

10.6 ACCOUNTABILITY

10.6.1 Responsibility for compliance with this procedure

Staff members are responsible for reading and complying with this procedure and any associated policies, procedures, guidelines or conditions of use.

All email sent outside the University must have the following disclaimer automatically attached.

"The information contained in this email and any attachments is confidential and may be legally privileged. If the recipient of this message is not the intended addressee, be advised that you have received this message in error and that legal professional privilege is not waived and you are requested to re-send to the sender and promptly delete this email and any attachments. If you are not the intended addressee, you are strictly prohibited from using, reproducing, disclosing or distributing the information contained in this email and any attached files.
Curtin University of Technology ("Curtin") advises that this email and any attached files should be scanned to detect viruses. Curtin does not represent or warrant that this email including any attachments is free from computer viruses or defects. Curtin shall not be responsible for any loss or damage incurred in use."

By logging on to the STAFF Domain, they accept this procedure and any published policies, procedures and conditions of use that apply to electronic facilities and services provided by the University.

11. PERFORMANCE INDICATORS

Indicators	Standard	Measures	Target	Method	Frequency	Responsible Owner	Undertaken by
System & Network availability	*% of time*	*Uptime*	*99.7% during teaching time*	*System report/log*	*Monthly*	*ICT Mgr*	*ICT Officer or Team Lead*

12. RESPONSIBILITIES (optional if responsibilities are already specified in the performance indicators)

Role (Position, Committee)	Accountable for

13. **APPENDICES (FORMS, WORK INSTRUCTION, SCHEDULES, PROCEDURES)** *(required if there are forms, work instructions related to the policy. May be created as a separate document)*

14. **OTHER RELEVANT DOCUMENTS/LINKS**

RESPONSIBILITIES	
Policy Manager	Manager of Information and Communication Technology
Contact Officer	Manager of Information and Communication Technology
Telephone	085 443998
E-mail	jdian@curtin.edu.my
Approval Authority	Chief Operating Officer
Date of Approval	**Feb 2008**
Assigned Review Period	3 years
Date of Next Review	22nd July 2019

REVISION HISTORY				
Version Number	*Approved/ Rescinded*	*Date Approved/ Rescinded*	*Resolution Number/ Minutes Reference*	*Reason for & Details of Amendment*
1.0	Feb 2008	15 March 2008	ICT Steering Committee	Initial ICT use policy and procedure
2.0	Approved	23/7/2015	RA/08/2015	Changes on the procedure that is not up to date and converted to the new template