INTERNATIONAL ISLAMIC UNIVERSITY

MALAYSIA

Policy for Responsible Use (staff)

IIUM ICT POLICY DOCUMENT

PREPARED FOR:
International Islamic University Malaysia

PREPARED BY:
Information Technology Division

Document Change Log

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0	23-JUL-2012		

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Dr. Basri Hassan, ITD	Initial Draft	01/07/2006	–
Adi Azmir Abdul Ghani, ITD	Reviewed	23/04/2008	–
Assoc Prof. Dr Abd Rahman Ahlan, ITD	Submission to ICT Committee No 2/2012	-	31/07/2012

1. OBJECTIVE

1.1 This policy describes the provision of information and communication technology resources by the IIUM and the responsibility of the when accessing these resources

1.2 The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

1.2.1. The ICT resources of the IIUM are provided to support the teaching and learning, research, consultancy and administrative activities of the University;

1.2.2. Staff are granted access to University resources, sensitive data and to external networks on the basis that their use of ICT resources shall be responsible, ethical and lawful at all times;

1.2.3. Staff are required to observe the University rules and regulations;

1.2.4. Data and information relating to persons and other confidential matters acquired for business purposes shall be protected;

1.2.5. University Business information shall be protected from unauthorized and/or accidental disclosure; and

1.2.6. University ICT resources must not under any circumstances be used to humiliate, intimidate, offend or vilify others on the basis of their race or gender.

1.3. This policy, to which all staff should adhere, identifies what is acceptable use including the personal use of ICT resources.

1.4. This policy identifies the possible consequences should a breach of the policy occur

2. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the "University"
ICT	Information and Communication Technology
ITD	Information Technology Division

3. POLICY STATEMENTS

3.1. ICT Resources

These resources cover all ICT facilities including the IIUM network, computers, computing laboratories, all associated networks in classrooms, lecture theatres and video conferencing rooms across the University, internet access both wired and wireless, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the University), telephone services and voicemail.

3.2. Access to ICT Resources

This policy prescribes the conditions under which access to IIUM ICT resources is granted.

3.2.1. Lawful Use

The use of ICT Resources must be lawful at all times. Unlawful use will breach this policy and will be dealt with as a disciplinary offence.

Unlawful use of ICT Resources may also lead to criminal or legal action being taken against the staff.

The University will not defend or support any authorized user who uses ICT resources for an unlawful purpose.

3.2.2. Granting of Access and Entitlement

Access to ICT Resources is approved by the relevant authority. Access is normally given based on a need to access that ICT Resource and is subject to the availability of those resources.

3.2.3. Non-Disclosure

Users may be required to sign a Non-Disclosure agreement prior to authorization being granted for access to certain ICT Resources.

3.2.4. Access on contract expiry or authorized access period

Email and computer access will cease on expiration of contract or services. For strictly professional or work-related reasons, staff and other authorized users may request that computer access be extended for a period of up to 30 days. Approval must be given by the Dean/Director of local entities and the Director of the ITD.

3.2.5. Responsibilities Regarding Use of University Computer Accounts

Each authorized user is responsible for:

- The unique computer accounts which the University has authorized for the user's benefit. These accounts are not transferable.
- Selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer.

3.2.6. Restrictions to Access

Users are forbidden unauthorized access to accounts, data or files on IIUM ICT Resources or any other ICT resource. The Administrator of an ICT Resource may restrict access to an individual user on the grounds that the user is in breach of this policy.

3.2.7. Third Party Access

Entities other than the ITD may neither negotiate nor grant third parties access to the University’s applications, databases, communications and network infrastructure.

3.2.8. Domain Name Registration

All domain names for IIUM projects/activities must be registered through the Director of the ITD. This requirement must be observed in all instances. Users should note that it is the University who owns and controls the site and not the person who registers the name.

3.2.9. Software License Restrictions

Use of licensed software is subject to terms of license agreements between the IIUM and the software owner or licensor, and may be restricted in its use.

3.3. Personal Use of ICT Resources

3.3.1 Extent of Personal Use

An authorized user is permitted to use the ICT Resources for limited, incidental personal purposes. Personal use of the ICT Resources is permitted provided such use is lawful, does not negatively impact upon the user’s work performance, hinder the work of other users, or damage the reputation, image or operations of the University. Such use must not cause noticeable additional cost to the University.

3.3.2 Commercial Use

ICT Resources must not be used for private commercial purposes.

3.3.3 University Liability

The University accepts no responsibility for:

Loss or damage or consequential loss or damage, arising from personal use of the University's ICT Resources;

Loss of data or interference with personal files arising from the University's efforts to maintain the ICT Resources.

3.4 Internet, Email and Messaging

3.4.1 Access to the Internet

Work Purposes

Authorized users are permitted to access the Internet for work related purposes.

Personal Use

Access is also permitted for personal purposes provided such use is lawful and reasonable in terms of time and cost to the University.

3.5. Personal Web Pages

3.5.1. Publication of Personal Web Pages

Staff is permitted to publish personal web pages on computers connected to the IIUM network. The content of material on personal web pages sites must be in accordance with any written law of the country.

The University reserves the right to regularly monitor personal web page sites hosted on IIUM servers, and to remove material, or request the user to remove or alter the content on their personal web page should it be inconsistent with any of the above.

Special care must be taken with web pages so as not to infringe any third party copyright in an audio or video file, music charts/lyrics, photographs or text.

3.5.2. Disclaimer Required on Personal Web Pages

A personal web page site must carry the IIUM Personal Page Disclaimer as a standard disclaimer on every page. The disclaimer states that the web page site is not authorized by the IIUM and that any opinions expressed on the pages are those of the author and not those of the University.

3.5.3. Responsibility for Personal Web Pages

Legal responsibility for personal pages rests with the user. The University will not defend a user named in an action arising from material published on a personal web site and will not be liable for any damages awarded against the user by a court or commission.

3.6 Email and Messaging

3.6.1 User Responsibilities

When using the email or messaging system, users must at all times:

- Respect the privacy and personal rights of others;
- Take all reasonable steps to ensure copyright is not infringed;
- Take all reasonable care not to plagiarize another person's work; or defame another person;
- Not forward or otherwise copy a personal email (except with permission of the author) or an email which contains personal information or an opinion about a person whose identity is apparent (except with permission of that person);
- Not send forged messages, or obtain or use someone else's e-mail address or password without proper authorization;
- Not send mass distribution bulk messages and/or advertising without approval of the user's Head of Department, or Administrative Head;
- Not send SPAM. The user must ensure that the recipient(s) of the intended email has/have consented to receive such email(s);
- Not harass, intimidate or threaten another person or other persons:
- Not send sexually explicit material, even if it is believed that the receiver will not object.

3.6.2 Standards Required When Using Email

- The private commercial use of email and messaging is not allowed and appropriate standards of civility should be used when using email and other messaging services to communicate with other staff members, students or any other message recipients.
- When using the email or messaging system, users must not send:
    - Angry or Antagonistic Messages – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures;
    - Offensive, Intimidating or Humiliating Emails - University ICT Resources must not be used to humiliate, intimidate or offend another person or other persons on the basis of their race, gender, or any other attribute prescribed under the University and Malaysian anti-discrimination legislation.

3.7 Security of ICT Resources

3.7.1 Staff's Responsibilities

A staff is responsible at all times to:

- Act lawfully.
- Keep all ICT Resources secure.
- Not compromise or attempt to compromise the security of any ICT Resource belonging to the University or other organizations or individuals, nor exploit or attempt to exploit any security deficiency.
- Take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, and protection from theft.
- Ensure the computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information.

3.7.2 Confidential Information

A staff is responsible at all times to:

Staff has a duty to keep confidential:

- All University data unless the information has been approved for external publication; and
- Information provided in confidence to the University by other entities.
- Each staff member is under the obligation not to disclose University business information unless authorized to do so. Breach of confidentiality through accidental or negligent disclosure may expose a user to disciplinary action.

3.8 Prohibited Use of ICT Resources

3.8.1 Advertising and Sponsorship

Paid advertisements are not permitted on any website using an IIUM domain name, personal website or any website, which has a substantial connection with the University except with the written permission of the University authority.

3.8.2 Unauthorized Access

Users are expressly forbidden from gaining unauthorized access or attempting to gain unauthorized access to ICT Resources belonging to the University and other organizations.

3.8.3 Peer-to-Peer File Sharing (P2P)

Installation or use of peer to peer file sharing software is not permitted on the IIUM network. Exceptions for legitimate teaching or research use must be approved by the University authority.

3.8.4 Pornography

Users are not permitted to utilize the University's ICT Resources to access , create, store or distribute pornographic material of any type.

3.8.5 Gambling

Users are not permitted to utilize the University's ICT Resources to gamble.

3.8.6 Computer Games

Users are not permitted to utilize the University's ICT Resources to play computer games during normal office hours.

3.9 Privacy and Surveillance

3.9.1 Security and Privacy

The accounts, files and stored data including, but not limited to, email messages belonging to users at the University are normally held private and secure from intervention by other users, including the staff of the Information Technology Division.

There are situations in which duly authorized ITD staff may be required to intervene in user accounts, temporarily suspend account access or disconnect computers from the network in the course of maintaining the University's ICT Resources such as repairing, upgrading or restoring file servers or personal computer systems.

Users should be aware that ITD staff may from time to time become aware of the contents of user directories and hard disk drives in the normal course of their work, and they are bound to keep this information confidential.

3.10 Access to and Monitoring of Equipment

The University does not generally monitor email, files or data stored on University ICT resources or traversing the University network. However, the University reserves the right to access and monitor any computer or other electronic device connected to the IIUM network. This includes equipment owned by the University and personal computing equipment (e.g. laptops) that are connected to the network.

Access to and monitoring of equipment is permitted for any reason, including, but not limited to, suspected breaches by the user of his/her duties as a staff member, unlawful activities or breaches of University legislation and policies. Access to and monitoring of equipment includes, but is not limited to email, web sites, server logs and electronic files. The University may keep a record of any monitoring or investigations.

3.11 University Liability

The University accepts no responsibility for:

- The loss or damage of a staff's property, arising from the use of the University's ICT Resources.
- The Loss of data or interference with files arising from the University's efforts to maintain the ICT Resources.

4. IMPLEMENTATION AND NON-COMPLIANCE

4.1 The Director of Information Technology Division holds the responsibility for the implementation of this policy and shall take necessary actions in the event of violation of this policy.

4.2 Alleged or suspected violations of the "Responsible Use of ICT Resources - Staff" should be reported to the Director of the Information Technology Division. Abuse of ICT privileges is subject to disciplinary action, which may include the loss of these privileges.

5. ENTITIES AFFECTED BY THIS POLICY

5.1 All staff is affected by this policy.

6. MAINTENANCE OF POLICY

6.1 The Information Technology Division is responsible for the formulation and maintenance of this policy.

7. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

7.1 ICT Regulations 2012

7.2 ICT Security Policy