

ICT POLICY

Approved by	Razali Mahfar
Date	
Effective Date	8 March 2007
Version:	1.0

Table of Contents

1.	INTRODUCTION	3
2.	PURPOSE	3
3.	SCOPE OF DOCUMENT	4
4.	RESPONSIBLE AUTHORITIES	5
5.	POLICY STATEMENTS	6
5.1.	GENERAL	6
5.2.	ACCEPTABLE USE	6
5.3.	PERSONAL USE	8
5.4.	PROHIBITED USE (UNACCEPTABLE USE)	8
5.5.	PREVENTION, DETECTION & INVESTIGATION OF MISUSE	11
6.	LEGISLATION	12
6.1.	COPYRIGHT ACT 1987	12
6.2.	COMPUTER CRIMES ACT 1997	12
6.3.	DEFAMATION ACT 1957	12
6.4.	OBSCENITY - THE COMMUNICATIONS AND MULTIMEDIA ACT 1998	13

1. INTRODUCTION

- 1.1 This document defines the policy of the International Centre of Education on Islamic Finance (INCEIF) in respect of the acceptable use of its information and communications technology (ICT) resources.

2. PURPOSE

- 2.1 The ICT Unit is responsible, on behalf of INCEIF, for reducing and managing potential risks to INCEIF and its associates, both operational and legal, from the consequences of the misuse of its ICT resources.
- 2.2 The policy has been established in order to:
 - 2.2.1 Protect INCEIF's investment in ICT resources,
 - 2.2.2 Provide INCEIF with a controlled and secured integrated ICT environment to support the business operations' needs and to enable seamless flow of information across the organisation,
 - 2.2.3 Protect the security, privacy and confidentiality of data and information within the ICT environment,
 - 2.2.4 Reduce INCEIF's business and legal risks, and
 - 2.2.5 Define the responsibilities and requisites for the use of ICT resources within INCEIF's environment.
- 2.3 In summary, the purpose of this policy is therefore to define clearly both users' obligations in using INCEIF's resources, and the ICT Unit's responsibility and authority in taking action to safeguard them.
- 2.4 This policy may be implemented either independently or to complement any existing policies put in place by individual divisions or departments, provided that in the event of any inconsistencies, this policy shall prevail.

3. SCOPE OF DOCUMENT

- 3.1 This policy applies to all students, staff, consultants, contractors, authorised guests and other authorised IT Users at INCEIF (referred henceforth in this document collectively as 'Users').
- 3.2 This policy defines the Acceptable Use, Personal Use and Prohibited or Unacceptable Use of INCEIF's ICT resources, which includes (but are not restricted to):
 - 3.2.1 Firmware, Software and databases, including (but not exclusively) applications and information systems, virtual learning and videoconferencing tools, electronic journals & e-books, software tools and ICT related services.
 - 3.2.2 Computing hardware, both fixed and portable, including (but not exclusively) servers, personal computers, workstations, laptops, UPS, PDAs, printers, scanners, disk drives, monitors, keyboards, tablets and pointing devices, thumb-drives.
 - 3.2.3 Network infrastructure, including (but not exclusively) the physical equipment and infrastructure, whether wired or wireless, such as network servers, cables, firewall, connections, switches and routers.
 - 3.2.4 Network services, including (but not exclusively) Internet access, web services, email, wireless services, messaging, telephony and fax services (VOIP).
- 3.3 This policy will:
 - 3.3.1 Provide guidance about acceptable and unacceptable use of ICT resources provided by INCEIF, as defined in clause 3.2.
 - 3.3.2 Establish a framework within which Users can apply self-regulation to their use of ICT resources.
 - 3.3.3 Describe the standards of which Users are expected to diligently observe when using ICT resources, and ensures that Users are aware of the legal consequences attached to inappropriate use of these resources.
 - 3.3.4 Advise Users that their usage of INCEIF ICT Resources is for official purposes only. And that their usage will be monitored and, in some cases, recorded.
 - 3.3.5 Specify disciplinary actions that INCEIF will take in the investigation of complaints received from both internal and external sources on any unacceptable use of INCEIF's ICT resources.

4. RESPONSIBLE AUTHORITIES

- 4.1 The term “Designated ICT Unit Authority “ used in this policy means the Chief Operations Officer (COO) or his authorised designate. This policy is issued under the authority of the COO who as a senior Officer of INCEIF is responsible for enforcing sanctions where necessary to safeguard INCEIF and its members.
- 4.2 The IT Infrastructure and resources are managed by the ICT Unit Manager, who is responsible for the prevention and detection of ICT misuse.
- 4.3 This policy is managed by the ICT Unit Manager who is responsible for investigating incidents of ICT misuse.

5. POLICY STATEMENTS

5.1. GENERAL

- 5.1.1 For the security and benefit of INCEIF and its Users, any person using ICT resources must abide by the Policy set henceforth. This Policy may be requested from ICT Unit (IU) to ensure that ICT resources are not abused.
- 5.1.2 It is the policy of INCEIF to:
 - 5.1.2.1 Provide a working environment that encourages access to knowledge and sharing of information.
 - 5.1.2.2 Maintain ICT resources for academic and administrative purposes that provide access to its community for local and worldwide sources of information.
- 5.1.3 INCEIF retains the right to monitor a selection of messages and materials sent across or stored in computers or storage areas managed by INCEIF and to take any appropriate action if it comes its attention that access to ICT resources is being abused or misused.

5.2. ACCEPTABLE USE

- 5.2.1 It is INCEIF's policy that:
 - 5.2.1.1 INCEIF's ICT resources are provided in support of INCEIF's teaching, learning, research, enterprise, and administrative activities.
 - 5.2.1.2 They may be used for any purpose that is in accordance with the aims and policies of INCEIF including inter-working with other institutions / organisations.
 - 5.2.1.3 Only registered users (i.e. those holding valid usernames and passwords) or those given permission by the designated authority are permitted to use INCEIF's ICT resources.
 - 5.2.1.4 Users can have full access only to their own information, or the information that are publicly available, or to which they have been given authorised access.
 - 5.2.1.5 Users may only use ICT resources that they are authorised to use and only for the approved specified purposes for which their accounts were issued.
 - 5.2.1.6 Users are expected to:
 - 5.2.1.6.1 Be prepared to show IU staff their Identity Card (ID) card as proof of identity when requested.
 - 5.2.1.6.2 Treat INCEIF's ICT Resources with care and use only in accordance with the proper operating instructions.
 - 5.2.1.6.3 Protect their account access (login) ID, password from unauthorised use. Users who share their login access with other individuals shall be responsible and will be held accountable for activities generated via their accounts.
 - 5.2.1.6.4 Respect the published times of access to the resources, where applicable.

- 5.2.1.6.5 Respect the rights of others, and conduct themselves in a quiet orderly manner when using the open access resources, and by complying with all INCEIF policies regarding sexual, racial and other forms of harassment, as well as by protecting the privacy of personal data to which you have access.
- 5.2.1.6.6 Comply with all valid regulations and legislation covering the use of Copyright and licensed material, including software, whether those regulations are made by law, or the originator of the material, or the distributor of the material, or INCEIF, or by any other legitimate authority.
- 5.2.1.6.7 Make all reasonable efforts to send data that is 'Virus Free', and to protect themselves from viruses and hacking attempts when connected to INCEIF's network either on or off Campus. INCEIF will not be held responsible for any damage to users' systems or information that occurs through such virus or hacking attacks.
- 5.2.1.6.8 Conform to all other appropriate policies and guidelines from IU and INCEIF.
- 5.2.1.6.9 Abide by any additional conditions imposed by providers of external ICT facilities when using any of INCEIF ICT resources to legally access any authorized external network and/or computer resources related to their work or for the performance of their duties and obligations to INCEIF.
- 5.2.1.6.10 Promptly report any incidents of possible abuse or misuse of ICT Resources, policy violations or weaknesses in INCEIF's ICT security.
- 5.2.1.6.11 Respect and adhere to any state or federal law, which may govern the use of information technology or communication networks.
- 5.2.1.6.12 Gain the basic knowledge in information technology through their own initiatives, especially on issues relevant to their basic ICT operational needs and for the purpose of understanding this Policy.
- 5.2.1.6.13 Manage their use of assigned / allocated ICT resources and are accountable for their actions related to ICT resources usage and security.
- 5.2.1.6.14 Learn about Internet etiquette, customs and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.

5.3. PERSONAL USE

- 5.3.1 INCEIF accepts that a User's Personal Use of INCEIF's ICT resources is within the scope of Acceptable Use, subject to the provisos within this document.
- 5.3.2 It is the policy of INCEIF that personal use will normally be tolerated provided that the personal use:
 - 5.3.2.1 Is occasional and reasonable and does not interfere with, nor detract from an individual's everyday workload and commitments nor with the effective functioning of INCEIF or any part of it.
 - 5.3.2.2 Complies with all other terms of this ICT Policy.
 - 5.3.2.3 Must not be of a nature that competes with INCEIF's business.
 - 5.3.2.4 Must not be of a commercial or profit-making nature, or for any other form of personal financial gain, unless prior written approval is obtained from INCEIF
- 5.3.3 Users must NOT add, or install their personal ICT software or hardware to INCEIF ICT resources without the appropriate management authorisation.
- 5.3.4 Users are expected to seek advice and guidance of the ICT Unit personnel if they are in any doubt on what constitutes acceptable and appropriate with regards to the personal use of ICT resources.
- 5.3.5 INCEIF reserves the right to withdraw access to ICT resources for this category of use at any time.

5.4. PROHIBITED USE (UNACCEPTABLE USE)

- 5.4.1 It is the policy of INCEIF to prohibit the use of its ICT resources when used or attempted to be used intentionally in contravention of the general principles outlined in 5.1 above.
- 5.4.2 The activities prohibited under this policy include (but are not restricted to) those listed below. Users must not:
 - 5.4.2.1 Damage or undermine the good name & reputation of INCEIF or any part of it;
 - 5.4.2.2 Access, create, change, store, download or transmit material which INCEIF may deem to be threatening, defamatory, abusive, indecent, obscene, racist or otherwise offensive;
 - 5.4.2.3 Place links to websites which have links to, or displays pornographic and inappropriate material, facilitate illegal or improper use, or to bulletin board which are likely to publish defamatory materials or discriminatory statements; or where copyright protected works such as computer software or music are unlawfully distributed;
 - 5.4.2.4 Create or transmit any offensive, excessively violent, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
 - 5.4.2.5 Generate excessive noise, cause annoyance, inconvenience or needless anxiety to, or to violate the privacy of, anyone else in the usage of ICT resources;
 - 5.4.2.6 Allow the ICT resources to be damaged or contaminated by food, drink or smoking materials;
 - 5.4.2.7 Interfere with the legitimate use by others of the ICT resources, or interfere with or remove computer printout or media belonging to others;

- 5.4.2.8 Send unwanted e-mail, chain and / or Spam letters, hoax virus warnings, pyramid letters or similar schemes using INCEIF e-mail or other electronic messaging system;
- 5.4.2.9 Falsify E-mails to make them appear to have been originated from someone else;
- 5.4.2.10 Make use and possess, distribute, sell, hire or otherwise deal with any unauthorised copies of computer software for any purpose without the license of its owner;
- 5.4.2.11 Install any software that is not licensed to INCEIF and /or install without authorisation, software licensed to INCEIF on any of INCEIF's computer systems under any circumstances, even if such software is used or is intended for carrying out of official work, duties and responsibilities of INCEIF;
- 5.4.2.12 Transmit unsolicited unauthorised commercial or advertising material;
- 5.4.2.13 Use the ICT resources for commercial, social or group distribution activities unless permission has been formally granted by the Designated ICT Unit Authority;
- 5.4.2.14 Gain unauthorised personal commercial benefit;
- 5.4.2.15 Use ICT resources as a staging ground or platform to gain unauthorised access to resources or services via INCEIF network; In particular, the confidentiality of data belonging to other Users must be respected.
- 5.4.2.16 Allow others to gain such unauthorised access, either willfully by disclosing user names or passwords or neglectfully by failing to log out of the system, thereby permitting unauthorised use of an INCEIF account;
- 5.4.2.17 Attempt to circumvent or subvert systems, networks, or resources of the Internet, destroy the integrity of computer-based information, or access controlled information and/or systems without formal authorization;
- 5.4.2.18 Conduct activities that might interfere with the operational performance and/or integrity of INCEIF ICT resources, including playing games, listening or viewing streaming audio/video for recreation, and intentionally running programs that attempt to violate the operational integrity of ICT resources;
- 5.4.2.19 Use ICT resources for partisan political purposes, such as using electronic mail to circulate advertising for political candidates or lobbying of public officials.
- 5.4.2.20 Use ICT resources for engaging in any outside fund-raising activities, including non-profit activities, endorsing any products or services, participating in any lobbying activities;
- 5.4.2.21 Disseminate any material which may incite or encourage others to carry out unauthorised access to or unauthorised modification of the INCEIF's or others' computer resources or materials;
- 5.4.2.22 Introduce and transmit material (including, but not restricted to, computer viruses, Trojan horses and worms) designed to be destructive to the correct functioning of computer systems, software, networks and data storage, or attempt to circumvent any precautions taken or prescribed to prevent this;
- 5.4.2.23 Attempt to circumvent INCEIF's firewall systems, or use file-sharing systems (sometimes known as P2P or peer-to-peer) without first gaining the permission of the designated authority;
- 5.4.2.24 Change, damage, dismantle, corrupt, or destroy (or cause to be changed, damaged, dismantled, corrupted or destroyed) any network component, equipment, software or data, or its functions or settings, which is the property of INCEIF, its partners, staff, students, visitors, or anyone else, without the express permission of the Designated ICT Unit Authority;

- 5.4.2.25 Cause any of INCEIF's ICT services to be overloaded, impaired, disrupted, curtailed or denied (other than in compliance with the direct instruction of the Designated ICT Unit Authority);
- 5.4.2.26 Connect any non approved computer network equipment (including wireless access points) to the INCEIF network without first gaining the written permission of the Designated ICT Unit Authority;
- 5.4.2.27 Set up any network services (e.g. web servers, e-mail services etc) unless formally sanctioned by the Designated ICT Unit Authority;
- 5.4.2.28 Register any domain name which includes the name of INCEIF or any name which may mislead the public into believing that the domain name refers to INCEIF;
- 5.4.2.29 Continue to use any item of networked hardware or software after a Designated ICT Unit Authority has requested that use ceases because of its causing disruption to the correct functioning of INCEIF ICT resources, or for any other instance of Unacceptable Use;
- 5.4.2.30 Fail to comply with any action directed by a Designated ICT Unit Authority to prevent or respond to any threats to the correct functioning of INCEIF's ICT resources;
- 5.4.2.31 Contravene the local rules for INCEIF ICT resources outside IU;
- 5.4.2.32 Create or transmit material that infringes the copyright of another person or institution, or infringe the Copyright laws of the Malaysia and other countries;
- 5.4.2.33 Interfere with the legitimate activities of other users covered within the principles outlined in Section 5.2 of Acceptable Use;
- 5.4.2.34 Otherwise act against the aims and purposes of INCEIF as specified in its rules, regulations, policies, and procedures adopted from time to time
- 5.4.2.35 Contravene applicable laws and prevailing regulations and policies applied by bodies external to INCEIF.
- 5.4.2.36 Use ICT resources for posting INCEIF's information to external newsgroups, bulletin boards or other public forums without authority, including information, which is at odds with INCEIF missions or positions. This includes any use that could create the perception that the communication was made in one's official capacity as an employee of INCEIF;
- 5.4.2.37 Use login credentials that do not belong to them.

5.5. PREVENTION, DETECTION & INVESTIGATION OF MISUSE

- 5.5.1 Access to INCEIF ICT resources is a privilege subjected to appropriate use. The ICT Unit shall investigate and review all complaints or instances of unacceptable use brought to their attention. Suspected or known abuse or misuse of ICT resources may result in disciplinary actions being taken against the offender. The severity of the disciplinary action shall be at the discretion of the Senior Management of INCEIF.
- 5.5.2 Where misuse of ICT resources has been identified, the matter will be investigated under INCEIF's appropriate disciplinary procedure. As an officer of INCEIF, the IT Manager or his nominee has the authority to investigate cases of alleged misuse and where applicable to apply sanctions directly, or to refer individuals to the Chief Academic Officer (for students) or to the Chief Operations Officer and the Human Resource Unit (for staff) for disciplinary action.
- 5.5.3 Any misuse which is in contravention of the law and/or which involves the intentional access, creation, storage or transmission of material which may be considered indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of INCEIF's official processes for dealing with academic ethical issues) will be regarded as an act of gross misconduct.
- 5.5.4 Students may be expelled for gross misconduct under INCEIF's student disciplinary procedures and staff may be dismissed under INCEIF's staff disciplinary procedures.
- 5.5.5 Where there is evidence of a criminal offence, the issue will be reported to the Police for them to take action. INCEIF will co-operate with the Police and other appropriate external government agencies in the investigation of alleged offences.
- 5.5.6 INCEIF retains the right to monitor or intercept any system logs, web pages, E-mail messages, network account or any other data on any computers system owned by INCEIF and to access all information held on its information and communications resources. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and INCEIF policies, or to secure effective system operation.
- 5.5.7 INCEIF reserves the right to inspect and validate any items of INCEIF owned computer equipment connected to the network. Any other computer equipment connected to the INCEIF's network can be removed if it is deemed to be interfering with the operation of the network.
- 5.5.8 It is the policy of INCEIF:
 - 5.5.8.1 To publish and promote its ICT Policy to all users of the INCEIF Network and to provide advice to users, on request, on matters relating to acceptable use
 - 5.5.8.2 To take effective and prompt action within existing disciplinary and / or legal frameworks against anyone found to be intentionally abusing the ICT resources.
- 5.5.9 In all cases where there is the potential for INCEIF's ICT resources to be abused, it is INCEIF's policy to:
 - 5.5.9.1 Record the identity of the individual using the specific resource at any given time.
 - 5.5.9.2 Retain these records and shall make them available to those authorized personnel appointed by INCEIF to investigate complaints of misuse.
 - 5.5.9.3 Destroy these records after twelve calendar months from the date of completion of investigations.

6. LEGISLATION

6.1. COPYRIGHT ACT 1987

- 6.1.1 The Copyright ACT 1987 is applicable to all types of creations, including text, pictures, graphics and sounds by an author or artist; including any that are accessible through INCEIF's ICT resources. For more information see:
http://www.kpdnhep.gov.my/index.cgi?action=pub&pub=act_1987
- 6.1.2 INCEIF Users must not infringe the Copyright laws of the Malaysia and other countries. Downloading files, music, films, TV programs, documents, licensed software and other material from the Internet carries the risk of infringing copyright. This applies to material illegally copied in Malaysia or elsewhere and then transmitted to another country via the Internet, will also infringe the copyright laws of the country receiving it.
- 6.1.3 Any uploading or downloading of information through on-line technologies that is not authorised by the copyright owner will be deemed to be an infringement of her/his rights.
- 6.1.4 Users must not make, transmit or store an electronic copy of copyright material on INCEIF's ICT resources without the permission of the owner.

6.2. COMPUTER CRIMES ACT 1997

- 6.2.1 It is a criminal offence to interfere with any computing system provided in the interests of health and safety and to gain unauthorised access to a computer system to make any unauthorised amendments of computer material (including the introduction of a computer virus).
- 6.2.2 The Act deals with three key crimes, namely unauthorised access to computer material, unauthorised modifications, and wrong communication. The Act applies within and outside the country as well as to any person regardless of his nationality or citizenship. For more information see http://www.msc.com.my/cyberlaws/act_computer.asp.

6.3. DEFAMATION ACT 1957

- 6.3.1 Defamation is a civil wrong, which in proven cases may incur substantial compensation.
- 6.3.2 Facts concerning individuals or organisations must be accurate, verifiable and views or opinions must not portray them and /or their subjects in any way that could damage their reputation.
- 6.3.3 Web pages and E-mail messages are regarded as published material. Legal responsibility will rest mainly with the sender of the email.
- 6.3.4 Check with INCEIF's Governance Unit before publicly displaying any contentious material.

6.4. OBSCENITY - THE COMMUNICATIONS AND MULTIMEDIA ACT 1998

6.4.1 Section 211 of the Communications and Multimedia Act 1998 states:

6.4.1.1 No content applications service provider, or other person using a content application service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

6.4.1.2 A person who contravenes section (1) commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand Ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day or part of a day during which the offence continued after conviction.

6.4.2 For more information on the Act, see http://www.msc.com.my/cyberlaws/act_communications.asp .