MINISTRY OF EDUCATION

ICT USAGE POLICY

Prepared by

Department of Information & Communication Technology
Ministry of Education
Jabatan Teknologi Maklumat dan Komunikasi
Kementerian Pendidikan

Date: May 2006

TABLE OF CONTENTS

ICT USAGE POLICY

1. Introduction

1.1. Background and Objectives

1.1.1. This document constitutes a policy for the management of ICT resources administered by MOE. The policy reflects the values of MOE and indicates, in general, what privileges and responsibilities are characteristic of the MOE ICT environment.

1.1.2. The primary intention of producing ICT usage within the MOE is to improve communications and increase efficiency amongst MOE employees.

1.1.3. The aim is to have secure and reliable ICT resources and the objective is to safeguard and maximise the usage of ICT resources.

1.2. Application and Scope of Policy

This Policy governs all use of MOE's network, computers, the Internet, and the e-mail system whether at the head office or remote offices. The policy applies equally to all MOE's employees granted access privileges to any Information Resource with the capacity to send, receive or store electronic mail; access the Internet and Intranet or both.

1.3. Official business

The computers, the network, the Internet and the e-mail system, including facsimile machines and voice mail supplied to you are for official business only. All information created, sent or received via the computer, e-mail system, network, and Internet is the property of MOE.

1.4. Confidentiality

MOE will treat information (this includes e-mail and electronic files) stored on computers as confidential (whether or not that such information is protected by the computer operating system). Requests for disclosure of information will be honoured only under one of the following conditions:

i. when approved by the appropriate ICT administrator;
ii. when authorised by the owners of the information;
iii. when required by the Laws of Brunei;
iv. except when inappropriate, ICT users will receive prior notice of such disclosures.

(Viewing of information in the course of system maintenance does not constitute disclosure).

1.5. Non-adherence.

In the event of non-adherence to the guidelines set out in the ICT Usage Policy or in the event of any legal consequences resulting from misuse or breach of any law MOE reserves the right to take necessary action which may include termination and/or legal action. Violations/misuse will be referred to MOE ICT department and will be dealt with in a serious and appropriate manner as stated further in Section 10.

1.6. Use of networks.

With respect to MOE policies the user is responsible for efficient use of the networks and facilities (public services) available to him/her. Use of MOE ICT resources must follow the guidelines of all the networks used.

1.7. Disclaimer

1.7.1 Since Internet is a global electronic network, there is no Ministry control of its users or content. Internet and its available resources may contain material of a controversial nature. MOE through its ICT staff cannot censor access to material nor protect users from offensive information. Head of departments will make every effort to ensure that obscene or 'undesirable' material will be removed from computer screens as soon as possible.

1.7.2 ICT staff cannot control the availability of information links which often change rapidly and unpredictably. Users need to be good information consumers, questioning the validity of the information.

1.7.3 MOE, in particular its ICT staff, assumes no responsibility for any damages, direct or indirect, arising from use of its WWW Server or from its connections to other Internet services.

1.8. Responsibility of Department

MOE will make every attempt to ensure that ICT users will adhere to the policies and procedures established by the MOE administrators. Every MOE department is responsible for managing their ICT resources and should appoint one IT coordinator to communicate with MOE ICT administrator (ICT department) to ensure that the policies are adhered to.

2. Definitions

"Artistic work" includes works of painting, drawing, sculpture (including casts and models) and artistic craftsmanship, and architectural works of art, and engravings and photographs;

"Computer" or "computers" means every ICT hardware and software supplied by the Government.

"Employee" means every public officer who is a holder of any public office or statutory body established by law and includes any person appointed to act in such office or statutory body;

"Government" means the Government of His Majesty the Sultan and Yang Di-Pertuan and shall include any public office or statutory bodies;

"ICT" means Information and Communications Technology;

"Literary work" includes maps, charts, plans, tables and compilations;

"MOE" means Ministry of Education;

"Official Business" means any tasks relating to role and responsibilities held as a public officer or staff of Government office;

"User" means any MOE users (employees and students) that is authorised to access the resource by the owner, in accordance with the owner's procedures and rules.

3. Computer Usage Policy

3.1. MOE Computers

All computers are property of MOE. Employees that violate these policies will be disciplined in accordance with MOE procedures. Employees that violate the policies are subject to disciplinary penalties which could include discharge and dismissal. It is to assure that computers are not used for unlawful purposes.

3.2. Login Access limitations

Login passwords are for personal use and are not to be distributed to anyone without expressed permission of the user or superior. Additionally, passwords do not create an expectation of privacy when it comes to employer monitoring internal and criminal investigations.

3.3. Computer related facilities violations and limitations

Use computer facility hardware and software appropriately. Violations include but are not limited to:

i. Disconnecting, reconnecting or reconfiguring hardware.
ii. Using the CD-writer or other media writer to copy software, music or other copyrighted media.
iii. Damaging or removing any property from the facility.

3.3.1. Interception or collection of password(s) by any means.

3.3.2. It is a misconduct to ask someone for their password, not even a system administrator needs to know someone's password. When a person's password is accidentally or inadvertently discovered, please immediately inform the password owner, so that they can change their password and adopt better security in the future.

3.3.3. Removing, changing or reconfiguring files on facility disks including hard drives.

3.3.4. Using another person's password that misleads message recipients.

3.3.5. A person should never give his/her password to anyone and should never allow anyone to use his/her user identification or e-mail account.

3.3.6. Using another person's computer account.

3.3.7. User should not access MOE e-mail account (individual) on other department's e-mail system. Users should open their e-mail account through Internet browser.

3.3.8. Probe or scan of ports on anyone's computer without authorisation from the owner of that computer is not allowed.

3.3.9. Disrupt the available services by performing any action that denies access of other users to the computing resources or adversely affects their use of the facilities. This includes:

i. Locking terminals (for long periods), holding up the printer queues; fetching and storing large files; and
ii. Playing any games on the computing systems.
iii. Downloading files through peer-to-peer internet sharing software.

3.3.10. Waste of computer resources is not allowed. For example:

i. Excessive printing.
ii. Frivolous inefficient computing.
iii. Attempting to crash operating systems.

3.4. Computing environment best practices

There are also a number of issues that are important for the maintenance of a reliable computing environment. Users should be aware and practice the following to ensure a reliable computing environment.

i. Neither food nor beverages are permitted near computer terminals, and ICT equipments.

ii. Use a surge suppressor to connect electric power and telephone lines to computer and peripheral equipment (printers, monitor and etc).

iii. Users should not switch off network hardwares (printer, computer and monitor) that are connected to a network, because it may cause failure of the network.

iv. Refrain from using pen drive for long periods of time or as permanent storage and backup, as this device is meant for transporting and sharing files only.

3.5. Use of Computers and its limitations.

3.5.1. Use of computers away from MOE sites includes but is not limited to home, car, hotel, hand phone, personal digital assistants, and other off-site locations.

3.5.2. Users should have no expectation of privacy when conducting office business at off-site locations. Additionally, users must adhere to all the same procedure restrictions as if they were using the computer at the office or school site when conducting office or school business.

3.5.3. All computers are to be used in a responsible, efficient, ethical and legal manner. Failure to adhere to the policy and the guidelines below will result in the revocation of the users' access privilege by the network administrator (ICT system administrator).

3.5.4. The person in whose name an account is issued is responsible at all times for its proper use.

3.6. General-Use of Computers

3.6.1. General-use computers are defined as computers, laptop, notebook, tablet PC, LCD projector and scanner that are used by many different departments each week.

i. Users should not install additional software on general-use computers.

ii. Users should not change preference settings in programs on general-use computers.

iii. Users should not print any documents using other MOE department printers and papers as this will affect department's resources. Instead users should make their own soft copy to print using their own resources.

3.6.2. Having food and drink in the office is a privilege. If food and drink spills are not cleaned up, food privileges will be revoked. If you are using a computer with greasy fingers, please wipe off the keyboard and mouse when you are done.

3.6.3. Users must respect that the office is a working space, and that people are concentrating. Use headphones to listen to music or broadcasts on the computers. Please use some common courtesy with regard to noise. If someone asks you to quiet down, do so.

3.7 Return of investment (ROI)

3.7.1 All MOE ICT resources must be used wisely and appropriately to maximize the return of investment.

3.7.2 ICT resources must be shared, where required, while not compromising the security of information.

3.7.3 All users assigned with ICT resources are responsible for the availability of these resources for official work at any time.

3.8 Usage of ICT resources by public.

3.8.1 For the approval of usage which does not involve payment, approval must be obtained from the Head of Department.

3.8.2 For approval for receiving payment from the usage of ICT resources, permission must be obtained from the Department of Administration and Services, Ministry of Education.

4. Copyright Protection

4.1. Definitions

Copyright is a property right that covers original literary, scientific, dramatic, musical or artistic works and other form of expression provided such works are fixed in a material or tangible form. Copyright does not subsist in a work unless the requirements of this Part with respect to qualification for copyright protection have been met.

4.2. Rights subsisting in copyright works

i. The owner of the copyright in a work of any description has the exclusive right to do the acts specified in Chapter II of the 'Constitution of Brunei Darussalam, Copyright Order, 1999' as the acts restricted by the copyright in a work of that description.

ii. In relation to certain descriptions of copyright work, the rights conferred by Sections 80, 83 and 88 of 'Copyright Order, 1999' subsist in favor of the author, director or commissioner of the work, whether or not he is the owner of the copyright.

4.3. Duration of Copyright

Copyright protection begins when the work (stated above) is actually created and fixed in a tangible form.

4.4. Authorship and Ownership of Copyright

A work of joint authorship means a work produced by the collaboration of two or more authors in which the contribution of each author is not distinct from that of the other author or authors.

4.5. Other applicable Copyright Act

For further Copyright policies users may observe and comply with the Copyright Order, 1999' currently in force by the Government of Brunei Darussalam.

5. E-mail Usage Policy

5.1. Expectation of privacy

In general, MOE, a representative of the Government as an employer can monitor e-mails at the office to ensure that they have a valid business purpose. So, policy can be a means to ensure that employees should have little or no expectation of privacy (as this will increase the likelihood of winning a privacy related lawsuit).

5.2. ICT ethics

Users are to use the ICT available to them in a responsible, effective and lawful manner in order to raise awareness of the consequences of irresponsible and unlawful use.

5.3. Registration and Termination

The administrator of email server (ICT administrator) is responsible for the creation and termination of email accounts for all MOE users.

5.4. Accessing E-mail Account
If there is a need of accessing other user's email account by a different user then that is the responsibility between the two (2) parties. This also applies to the 'leaving user' but it must be approved initially by their head of department.

5.5. E-mail rules

Employees are expected to follow the rules of etiquette and to produce messages that are effective and professional (e.g. formal letter). User should practice the following.

i. Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s).

ii. Any message or file sent via e-mail must have the employee's name, department's and/or units attached, explicitly revealing their identity.

iii. The use of personal e-mail accounts (such as hotmail) for official communications are not permitted unless expressly authorised in advance by MOE's systems administrator.

5.6. Sensitive information

User must not send classified or sensitive information through Internet or e-mail as it is difficult to control receiving messages.

5.7. Authorised external E-mail system

Receiving correspondence from vendors (private company) are only authorised through the company's email and Brunet's email system. Non e-mail accounts (e.g. Yahoo, Hotmail and email provided by other Internet Service Providers) are not permitted unless expressly authorised in advance by MOE's systems administrator.

5.8. Prohibited E-mail activities

The following activities are prohibited by policy:

i. Sending email with intent to harm a particular individual. Includes harassment, intimidation, threats, intentional infliction of emotional distress, defamation, obscene content, violations of privacy, disclosure or personal information (e.g. credit card numbers, medical history, etc) or insults directed at a specific person. If receiving such unsolicited messages delete them promptly and not forward them.

ii. Using e-mail for conducting personal business that is not related to the terms and reference of their work.

iii. Forging someone else's name to an e-mail.

iv. The use of unauthorised e-mail software.

v. Misuse of trademark(s) in e-mail and web pages. This includes MOE logo and trademarks owned by other organisations.

vi. Sending e-mail(s) that contain instructions or information for any unlawful activity (e.g. how to steal credit card numbers, intercept passwords to computer accounts, etc).

vii. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.

5.9. Prohibited activities in respect of network communications

The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

i. Sending or forwarding chain-type messages / e-mail and graphic files where they cause overload on MOE system.

ii. Sending excessively large messages exceeding 5 MB message at any time, or continuously over 24 hours to the same accounts with messages cumulatively exceed 20 MB.

iii. Sending unsolicited messages to large groups except as required by appropriate authority.

iv. Sending bulk e-mail is permissible when it is addressed to all members of MOE, when the content of the bulk e-mail is related to MOE business and relevant to the addressees.

v. Sending or forwarding e-mail that is likely to contain computer viruses, worms, malware (malicious software such as spyware and adware).

5.10. Retention Period

User should be aware of MOE's policies regarding e-mail retention periods of not more than 30 days. It is their responsibility to archive any messages that they do not wish to be automatically deleted.

5.11. Use of Non-Accredited Mobile Devices

User must not send, forward, receive or store confidential or sensitive information utilising non-accredited mobile devices (e.g. cellular and two-way pagers).

5.12. Standard Footer

User should at all times include the following footer as a standard:-

“This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity, to whom they are addressed. This communication may contain material protected by the Official Secrets Act (Cap 153) of the Laws of Brunei. If you are not the intended recipient or the person responsible for delivering the email to the intended recipient, delete this e-mail and attachment immediately”.

The standard footer (signature) for e-mails is left aligned. It should contain the following.

- Name
- Position
- Unit/Department
- Telephone No & Fax No.

5.13. Violations and Penalties

Any violations and penalties will refer to Violations and Enforcement section.

5.14 Spam email and network spamming activity

5.14.1 MOE email system is secured by anti-spamming software. All emails and contents of emails detected with spamming signatures are blocked from entering users mailbox. These emails will be quarantined by the system and checked by the system administrator for authenticity. Emails that are considered as authentic will be forwarded otherwise it will be deleted.

5.14.2 E-mail users who expected their email has been quarantined by the system should contact system administrator, stating the date of the email sent, the sender, and title of the email.

6. Internet and Intranet Usage Policy

6.1. Access Compliance

i. Files that are downloaded from the Internet must be scanned with virus detection software before being viewed or opened.

ii. All software used to access the Internet shall be configured to use MOE proxy.

iii. All sites accessed must comply with the MOE ICT Usage Policy.

6.2. Usage ethics

Employees may not use MOE's Internet or Intranet access for any of the following.

6.2.1 Prohibited Activities

i. Visiting sites featuring pornography, terrorism, espionage, theft or drugs, inciting racial hatred or disharmony.

ii. Online gambling or engaging in any other activity in violation of the laws of Brunei Darussalam.

iii. Conducting unauthorised business.

iv. Commercial uses. For example, sell or purchase anything over the Internet and disclose private information including credit card numbers.

v. Engaging in online subversive activities against the Government of Brunei Darussalam.

6.2.2 Downloading

i. No user may use the Internet facilities to propagate deliberately any virus.

ii. Download programs, which will significantly degrade the performance of the Internet facilities.

iii. Uses that cause harm to others or damage to their property. This includes, but is not limited to, any unauthorised modification of or deletion of another person's files or account.

6.2.3 Chats and newsgroups

i. Chats and newsgroups maybe used but solely for academic or office business purposes. Other purposes of chat are prohibited.

ii. Chats and newsgroups are public forums, therefore confidential department or personal information must not be revealed.

6.2.4 Auditing

ICT department may inspect any or all files that are stored on MOE resources to ensure a compliance with the MOE ICT usage policy.

6.3 Websites compliance

Websites and its contents must adhere to the following outlines;

i. Webpages contents, design and updating are the responsibility of the departments and institutions. Information must be updated frequently and relevant.

ii. Webpages contents and informations should express general rules of government regulations on information publication.

iii. Departments and institutions webpages should reside in the official MOE Webservers only.

iv. Naming convention for sub-domain and directories of Website must reflect their nature of subject and nature of business, and must consult system administrator in advance.

7. Network Policy

7.1. Network Connectivity

To ensure the security and integrity of information stored on the Government ICT system, employees accessing the Internet with a computer attached to Government's network must do so through an approved Internet connection. Accessing the Internet directly by modem is strictly prohibited, unless approved by network administrator.

7.2. Internet Service Provider (ISP)

Connections via other Internet service provider(s) to the government network are not permitted unless approved by ICT administrator.

7.3. Network access limitation

Employees may not use MOE's network access for any of the following:

i. Uses that jeopardise the security of access and of the network on the Internet.

ii. Accessing or attempting to access controversial or offensive materials.

iii. Uses that waste limited resources. For example, sending chain letters, e-mails, even for non-commercial or apparently 'harmless' purposes as these uses up limited network capacity resources.

iv. Use of MOE computer resources or electronic information without authorisation.

v. Making MOE computing resources available to individuals not affiliated with MOE without approval of authorised MOE officials.

vi. Unauthorised scanning of networks for security vulnerabilities is prohibited, unless it is authorised by ICT system administrator or their approved agent.

vii. Attempting to alter any MOE, computing or networking components (including bridges, routers and hubs) without approval of authorised MOE officials.

viii. Wiring including attempts to create network connections or any extension or re-transmission of any computer or network services unless approved by an authorised network administrator.

ix. Deliberate activities such as:

- Corrupting or destroying other users' data via the network
- Violating the privacy of other users via the network
- Disrupting the work of other users via the network
- Using the network in a way that denies services to other users
- Misuse of the network or network resources such as the introduction of 'viruses'

8. Software Policy

8.1. Licensed Software

MOE has licensed copies of computer software from a number of publishers to help fulfill its mission. Licensed and registered copies of software programs have been placed on computers within the organisation in accordance with the licensing agreements.

8.2. Software Copyright

No other copies of this software or its documentation will be made without the express written consent of the software publisher.

8.3. Software Copy

In some cases, the license agreements for a particular software program may permit an additional copy to be placed on a portable computer for business purposes. User will not make such additional copies of software or documentation for the software without verifying that a copy is permitted via the license agreement.

8.4. Software Distributor

ICT department will act as the coordinator for computer software licensing by assisting office units, institutions throughout MOE with purchases, installation, inventory and any required procedures necessary to ensure MOE compliance with applicable license and purchasing agreements.

i. Appointed vendors are allowed to install licensed software to every computer under MOE. Users may seek assistance from these appointed vendors if required.

ii. In the event of any damages related to the software, users are required to report it to ICT Department.

8.5. Copyright Violations

User who make, acquire or use unauthorised copies of computer software or documentation will be subject to disciplinary action including suspension or revocation of IT privileges.

8.6. Standards for software usage

Procedures for initial back-up copies of software are as follows.

i. All software, which is MOE property, must be copied prior to its initial use and the 'master' copy must be stored in a safe place.

ii. Master copies may not be used for ordinary on-going activities, but must be reserved for recovery from computer virus infections, hard disk crashes and other computer problems which render the original or installed copy unattainable or unusable.

8.7. Transfer and Recompiling Software

i. No user may sell, rent sublicense, lend, transmit, distribute, give or otherwise convey or make available software or an interest therein to any unauthorised individual or entity.

ii. No user shall recompile, disassemble or reverse-engineer any software except in those rare circumstances in which all applicable software licenses and agreements expressly permit it.

iii. No user shall reconfiguring software such as Mozilla to run unauthorised plug-ins.

iv. No user shall use software whose intent is to scan for vulnerabilities or gain unauthorised access to computers.

v. Users are not permitted to download, install or store any commercial, shareware or freeware software not related to your work, without prior approval from ICT system administrator (ICT Department).

8.8. Right to Audit

Not withstanding any privacy rights which might otherwise exist or apply:

i. MOE shall have the right to audit all resources to ascertain compliance with the MOE software policy, and

ii. MOE may permit the software licensors and their agents to audit some or all resources to ascertain compliance with their license, purchase or other applicable agreements.

8.9. Reporting Non-compliance

i. Any user who has questions about software use or the software policy shall promptly refer the question to ICT system administrator (ICT department).

ii. Any user who suspects an incident of non-compliance with the software policy by another user shall promptly notify the department director or ICT system administrator (ICT department).

9. Other related and applicable policies

In the use of the Computers, E-mail and the Internet, users must observe and comply with all other laws and regulations currently in force, as well as other policies or guidelines issued by the Government. The laws shall include but not limited to the following:

- Public Service Commission Act (Chapter 83)
- Official Secrets Act (Chapter 153)
- Constitution of Brunei Darussalam (Order under section 83(3) - Emergency (Copyright) Order 1999
- Constitution of Brunei Darussalam (Order under section 83(3) - Computer Misuse Order 2000
- Constitution of Brunei Darussalam (Order under section 83(3) - Electronic Transactions Order 2000
- Broadcasting Act (Chapter 180) - Internet Code of Practice
- Broadcasting Act (Chapter 180) - Broadcasting (Class License) Notification, 2001

10. Procedures for allegations of Misconduct

10.1. Litigation.

In the event of litigation, all computer users are on notice that Government civil rules of procedure may allow discovery of all computer hardware and software. This includes but is not limited to computers, laptops, home computers, printers, hand phones, and other electronic equipment that is used to conduct MOE business. Any attempt to damage or destroy evidence will evoke criminal actions.

10.2. Notification of Violations

If MOE believes unauthorised access to or disclosure of information has occurred or will occur MOE will make reasonable efforts to inform the affected computer account holder, except when notification is impractical or when notification would be detrimental to an investigation of a violation of policy.

11. Violations and Enforcement

11.1. Violations Referral

Any actual or suspected violation of the rules listed above should be brought to the head of department. In the case of serious violations, a report should be made to Chief Information Officer.

11.2. MOE response to a reported violation

i. Upon receiving notice of violation, MOE may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings.

ii. A person accused of a violation will be notified of the change and have an opportunity to respond before MOE imposes a permanent sanction. Appropriate cases will be referred to the MOE disciplinary authority appropriate to the violator's status.

iii. In addition to sanctions available under MOE polices, MOE may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks and other services or facilities.

iv. If MOE believes it necessary to preserve the integrity of facilities, user services or data it may temporarily suspend any account whether or not the account user is suspected of any violation. MOE will provide appropriate notice to the account user. Computers that threaten the security of MOE systems will be removed from the network and allowed to reconnect only with the approval of network administration.

11.3. Penalties

This may include but is not limited to temporary or permanent reduction or eliminations of access privileges or expulsion or terminations of service.

11.4. Serious Violations

If violations is serious and warrants action beyond the Ministry's imposed penalties, the case may be referred to Attorney General's Chambers for legal advice.

12. Amendments

This policy was adopted by the MOE on 9th August 2005. This procedure may be amended or revised from time to time as need arises. Users will be provided with copies of all amendments and revisions.

Employee Acceptance

I hereby acknowledge that I have read and understood the conditions outlined in this Information Resource Usage Policy and agree to abide by them.

Name :
Position :
Department :
E-mail :

Signature : Date:

Approved by Head of Department

Name :
Position :

Signature : Date:
(Official Stamp)

Action by (ICT Administrator)

Name :

Signature : Date:
(Official Stamp)

Acknowledgements

This leaflet, documents the acceptable use of computer systems, networks and other related facilities for Ministry of Education (MOE).

The Department wishes their utmost gratitude to the Director of Information and Communication Technology Department, the writer and ICT staffs for their support and encouragement in compiling the acceptable use of ICT Usage Policy.

Finally, a special thanks and greatest appreciation goes to the Law Senior Officer of Director General Office for her cooperation and support during the course of this policy.