TE MARAE ORA
MINISTRY OF HEALTH
COOK ISLANDS

INFORMATION & COMMUNICATIONS TECHNOLOGY (ICT) POLICY & PROCEDURES

JULY 2011

TABLE OF CONTENTS

1. INTRODUCTION

1.0.1 Major technological advances have resulted in sweeping changes to the way information is transmitted. Today the internet is an integral component of modern life. Internet browsing and email are the key method of written communication in scores of organizations – the Cook Islands Ministry of Health is no different.

1.0.2 The Cook Islands Health Strategy (2006) clearly articulates the need to focus on strengthening health infrastructure to ensure appropriate capacity exists to improve health outcomes for Cook Islanders. This includes providing for future health-sector development through the appropriate investment in information technology and telecommunication systems.

1.0.3 The Ministry of Health recognizes the importance of quality, efficient, user-friendly ICT systems in order to increase performance levels and provide excellent services to all Cook Islands health centers and patients. Freedom of speech and privacy principles creates important implications for email and internet services.

1.1. National Legislation and Policy

1.1.1 The National Information and Communication Technology Policy 2003 outline government's intention to develop national ICT policies and legislation. The rights and interests of individuals and communities must be balanced through compliance with the principles of good governance and transparency. The proposed regulatory framework will account for information security, confidentiality, privacy and intellectual property issues.

1.1.2 While positive steps towards achieving these goals have been taken – particularly the introduction of the 2008 SPAM Act – it is necessary for each government agency to proactively establish individual structures for ICT support. This is a core reason for the development of an ICT policy by the Ministry of Health, along with supporting guidelines for computer, email, and internet and phone usage.

2. SCOPE OF POLICY

2.0.1 The ICT network at the Ministry of Health is comprehensive and includes all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are:

2.0.1.1 controlled or operated by the Ministry of Health:
2.0.1.2 connected to the Ministry of Health network:
2.0.1.3 used at or for Ministry of Health activities:
2.0.1.4 brought onto a Ministry of Health site.

2.0.2 ICT includes but is not limited to; computers (such as desktops, laptops, PDAs), computer systems, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), telecommunication equipment, networks, databases and any other similar technologies as they come into use

3. POLICY STATEMENT

3.0.1 The purpose of this policy is to ensure an information technology infrastructure that promotes the values of the Ministry of Health and supports the Ministry of Health achieve its vision of '*Healthier Cook Islanders achieving their* aspirations'. The ICT policy governs the collection, management and dissemination of health information to guide the development of health policies and practice in the areas of patient care, community health and policy and planning. In particular, this Policy is:

3.0.1.1 To ensure the integrity, reliability, availability, efficiency and superior performance of ICT Systems;
3.0.1.2 To ensure that use of ICT Systems is consistent with the principles and values that govern use of other Ministry facilities and services;
3.0.1.3 To ensure that ICT Systems are used for their intended purposes; and
3.0.1.4 To establish processes for addressing policy violations and sanctions for violators.

3.0.2 This policy applies to all Ministry of Health ICT users (e.g. staff, contractors, students, consultants, etc), systems, applications and networks.

4. ICT SECURITY

4.0.1 The Ministry has made considerable investments into ICT resources. These must be protected by ensuring information held is kept secure and physical assets are cared for.

4.0.2 With patient data being held electronically, it is necessary to ensure the Ministry is kept protected from computer and software viruses which could potentially allow access to confidential data. Any protective measures taken must be frequently reviewed and updated. All equipment should also be password protected with access codes being changed at regular intervals.

4.0.3 The care of physical ICT assets is the responsibility of all Ministry employees. Permission should always be sought from a Manager or Director to temporarily remove such assets from Ministry property (e.g. taking laptops or cell phones home overnight). Any loss or damage to such ICT equipment is the employee's responsibility. Purchase of a similar asset of equal value or repair charges must be borne by the employee at fault.

5. ICT APPROPRIATE USE

5.0.1 Although this Policy sets out the general parameters of appropriate use of ICT systems, staff should also consult the Ministry's Personnel Policy and Procedures manual under Clause 8.3 for more detailed statements on permitted use and the extent of use that the Ministry considers appropriate in light of their varying roles within the community. In the event of conflict between ICT policies, this Appropriate Use Policy will prevail.

5.0.2 Under Clause 8.3 of the Ministry's Personnel Policy and Procedures manual, the provision of internet, email and computers to users are a requirement for the performance and fulfillment of responsibilities. However, use of these resources are limited to the parameters defined within the clause.

5.1. Acceptable /Appropriate Use

5.1.1. ICT systems may be used only for their authorized purposes that is, to support the clinical, administrative, and other functions of the Ministry of Health. The particular purposes of any ICT system as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user.

5.1.2. While the use of email distribution lists can be very effective, excessive use of email lists, especially with large messages, can cause congestion on network traffic. The forwarding of chain letters is considered to be spam and is not permitted.

5.1.3. The Ministry of Health recognizes that the Internet is an essential tool and as such the use of the Internet shall be treated as privilege given to those who have the approval of their respective Directors or Head of Ministry.

5.1.4. No one without specific authorization shall use any Ministry of Health computer or network facility for non-Ministry of Health business.

5.2. Systems Administration

5.2.1. Ministry of Health system administrators are entitled to remove from any Ministry of Health computing resource data and programs that are found to be inappropriate and/or to terminate the computing privileges of any user who violates the MOH ICT Policies.

5.3. Proper Authorization

5.3.1. Users are entitled to access only those elements of ICT systems that are consistent with their authorization.

5.4. Specific Restrictions on Use

5.4.1. The following categories of use are inappropriate and prohibited:

5.4.2. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

5.4.3. **Use that is inconsistent with the Ministry of Health's values and purposes**. The Ministry is a non-profit, government organization and, as such, is subject to public scrutiny and specific laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of ICT systems for non-Ministry purposes is prohibited, unless specifically authorized. Prohibited commercial use does not include communications and exchange of data that furthers the Ministry’s educational, administrative, research, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

5.4.4. **Use of ICT systems in a way that suggests Ministry endorsement of any political candidate or ballot initiative is also prohibited.** Users must refrain from using ICT systems for the purpose of political activities.

5.4.5. **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.

5.4.6. **Use that is damaging the integrity of Ministry or other ICT Systems**. This category includes, but is not limited to, the following activities:

5.4.6.1. **Attempts to defeat system security**. Users must not defeat or attempt to defeat any ICT system's security – for example, by "cracking" or guessing and applying the identification or password of another user, or compromising room locks or alarm systems. (This provision does not prohibit, however, Systems Administrators from using security scan programs within the scope of their Systems Authority.)

5.4.6.2. **Unauthorized access or use**. The Ministry recognizes the importance of preserving the privacy of users and data stored in ICT systems, particularly data related to patients. Users must honor this principle by neither seeking to obtain unauthorized access to ICT systems, nor permitting or assisting any others in doing the same. For example, people not employed by the Ministry of Health may not use Ministry ICT systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Ministry organizations or individuals across the Ministry network without specific authorization. Similarly, users are prohibited from accessing or attempting to access data on ICT systems that they are not authorized to access. Furthermore, users must not make or attempt to make any deliberate, unauthorized changes to data on an ICT system. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

5.4.6.3. **Disguised use**. Users must not conceal their identity when using ICT systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

5.4.6.4. **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

5.4.6.5. **Modification or removal of data or equipment**. Without specific authorization, users may not remove or modify any Ministry-owned or administered equipment or data from ICT systems.

5.4.6.6. **Use of unauthorized peripheral devices.** Without specific authorization, users must not physically, or use hardware specific cables (such as USB cables) to, attach any additional device (such as an external disk, printer, or video system) to ICT systems.

5.4.6.7. **Unauthorized use of network resources.** Users are not permitted to connect non-ministry laptops or workstations onto the Ministry's network without specific authorization.

5.4.6.7.1. **Use of antivirus scanning systems.** All authorized connectivity of non-ministry laptops and workstations to the Ministry of Health network must consent to the use of Ministry security scanning programs on these systems. Detection of security threats on these systems will result in immediate termination of privileges.

5.4.6.8. **Other prohibited uses.** Examples of such uses are: promoting a pyramid schemes; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making threats.

5.4.6.9. **Use in violation of law.** Illegal use of ICT systems that is, use in violation of civil or criminal law at the international or local level is prohibited.

5.4.6.9.1. Refer to the Cook Islands SPAM Act 2008.

5.4.6.9.2. With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

5.4.6.10. **Use in violation of Ministry contracts**. All use of ICT systems must be consistent with the Ministry's contractual obligations, including limitations defined in software and other licensing agreements.

5.4.6.11. **Use in violation of Ministry policy**. Use in violation of other Ministry policies also violates this policy. Relevant Ministry policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as Ministry policies and guidelines regarding incidental personal use of ICT systems.

5.4.6.12. **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

5.5. Free Inquiry and Expression

5.5.1. Users of ICT systems may exercise rights of free inquiry and expression consistent with the principles of the Ministry of Health and the limits of the law.

5.6. Personal Account Responsibility

5.6.1. Users are responsible for maintaining the security of their own ICT systems accounts and passwords. Any user changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their ICT systems accounts.

5.7. Responsibility for Content

5.7.1. Official Ministry information may be published in a variety of electronic forms. The Certifying Authority is responsible for the content of the published document.

5.8. Conditions of Ministry Access

5.8.1. The Ministry places a high value on privacy and recognizes its critical importance in a clinical setting. There are nonetheless circumstances in which, following carefully prescribed processes, the Ministry may determine that certain broad concerns outweigh the value of a user's expectation of privacy and warrant Ministry access to relevant ICT systems without the consent of the user. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

5.8.2. The Ministry may access all aspects of ICT systems, without the consent of the user, in the following circumstances:

5.8.2.1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the ICT systems; or
5.8.2.2. When required by law or administrative rules; or
5.8.2.3. When there are reasonable grounds to believe that a violation of law or a significant breach of Ministry policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
5.8.2.4. When such access to ICT systems is required to carry out essential functions of the Ministry; or
5.8.2.5. When required to preserve public health and safety.

5.9. Process

5.9.1. Consistent with the privacy interests of users, Ministry access without the consent of the user will occur only with the approval of the Secretary of Health and the user’s supervising Director as appropriate, or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The Ministry, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by the Director of Funding and Planning and Secretary of Health. A user will be notified of Ministry access to relevant ICT systems without consent; depending on the circumstances, such notification will occur before, during, or after the access, at the Ministry's discretion.

5.10. User access deactivations

5.10.1. In addition to accessing the ICT systems, the Ministry, through the appropriate Systems Administrator, may deactivate a user's ICT privileges, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the user of any such action.

5.10.2. Users will also have all their ICT privileges revoked upon retirement, resignation or termination from the Ministry of Health. The Systems Administrators will only proceed with user account deactivation once notification has been received from the Ministry's Human Resources Department on the user's employment status.

5.11. Logs

5.11.1. Most ICT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post policies and procedures concerning logging of user actions, including the extent of individually-identifiable data collection, data security, and data retention.

5.12. Reporting to Executives

5.12.1. To ensure that ICT services at the Ministry of Health is operating in accordance with legal and ethical requirements and accepted ICT practices, a quarterly report must be submitted to the Executives through the Director of Funding and Planning .

5.12.2. Activities that should be covered in the quarterly report is not limited to the following:

5.12.2.1. Policy and Planning
5.12.2.2. Systems Administration
5.12.2.3. Hardware Maintenance
5.12.2.4. Training and Development
5.12.2.5. Website Upgrade and Maintenance

5.13. Enforcement Procedures

5.13.1. Refer to the Ministry of Health Personnel Policy and Procedures document.

5.14. Further Development of Policy and Procedures

5.14.1. Additional ICT Policies to be developed:

5.14.1.1. Email Usage
5.14.1.2. Laptop Security
5.14.1.3. Security Classification
5.14.1.4. Computer and Network Security
5.14.1.5. ICT Security Compliance and Audit
5.14.1.6. Systems Procurement, Development and Maintenance Security

6. DEFINITIONS

ICT :
"ICT" means all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are:

a) controlled or operated by the Ministry of Health:
b) connected to the Ministry of Health network:
c) used at or for Ministry of Health activities:
d) brought onto a Ministry of Health site.

ICT includes but is not limited to; computers (such as desktops, laptops, PDAs), computer systems, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), telecommunication equipment, networks, databases and any other similar technologies as they come into use

User:
"User" means anyone who operates or interfaces with ICT. It includes Ministry of Health staff, officers and students (whether permanent, temporary or part-time), contractors, sub-contractors, consultants, business partners or official visitors or any other member of the Ministry of Health

Systems Authority:
While the Ministry of Health is the legal owner or operator of all ICT systems, it delegates oversight of particular systems to the head of a specific directorate or department ("Systems Authority"), or to an individual staff member, in the case of ICT systems purchased with funds for which he or she is responsible.

Systems Administrator:
Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular ICT resources.

Certifying Authority:
This is the Systems Administrator or other Ministry authority who certifies the appropriateness of an official Ministry document for electronic publication in the course of Ministry business.

Specific authorization:
This means documented permission provided by the applicable Systems Administrator or departmental manager.

SPAM
Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.