Internet Usage Guidelines
National Centre for Information Technology

Version 1
November 2009

1 Purpose

This document provides the standard for the use of the Internet by all government staff. The purpose is to provide a common guideline and remove inappropriate use of the Internet and strengthen the appropriate use of the Internet.

2 Scope

The guideline applies to all Government of Maldives agencies.

3 Internet Usage Guideline

3.1 Acceptable use

The following are specific provisions and guidelines regarding authorized use of Internet access and e-mail provided through government agencies:

1. Using Web browsers to obtain work-related/skill development information from Web sites.
2. Accessing databases for information as needed for research, study or education management.
3. Subscribing to distribution lists and other forms of e-mail subscription services related to education, research and or job function is allowed. If the service does not pertain to education, research or job function, manager's approval is required in writing before signing up.
4. Passwords are a user's best defence against unauthorized use of e-mail accounts. Do not compromise your account by giving it to others or displaying it in public view.
5. User should take care in addressing messages so it reaches the appropriate recipient. Also, spelling and grammar should be checked by the e-mail client before sending the message.
6. E-mail use must not interfere with the performance of study/work responsibilities.
7. The use of Internet Messaging, Chat programs and systems will require written permission from the manager
8. Abiding by existing national laws and regulations.

3.2 Unacceptable use

Users must not use the Internet for purposes that are illegal, unethical, harmful to the institution and institutions information systems and assets, or non-productive. Users shall not use Internet or e-mail services to view, download, save, receive, or send material related to the following:

1. Offensive content of any kind, including pornographic material.
2. Propagate a virus, worm, Trojan horse, or trap-door program code.
3. Disable or overload any computer system or network.
4. Use of social networking sites such as facebook or others during official working hours that impact the productivity
5. Circumvent any system intended to protect the privacy or security of another user.
6. Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
7. Visiting Web sites that promote threatening or violent behaviour.
8. Using the Internet for Illegal activities.
9. Distributing commercial messages.
10. Messages of a religious, political, or racial nature.
11. Gambling Web sites.
12. Downloading entertainment software, films or games
13. On-line Internet gaming

14. Personal financial gain.
15. Forwarding e-mail chain letters.
16. Downloading and distributing material protected under copyright laws without the proper consent of the owner.
17. Dispersing corporate data to the organization's customers or clients without authorization.
18. Opening files received from the Internet without performing a virus scan.
19. Make unreasonable use of personal e-mail accounts during official working hours
20. Use the network to sign up with websites or organizations that offer rewards, monetary or otherwise for surfing the internet.
21. Creating or exchanging offensive or obscene messages of any kind, including pornographic material.
22. Sending e-mail that promotes discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
23. Sending e-mail that contains a threatening or violent message.
24. Exchanging proprietary information, trade secrets, or other confidential information to anyone not affiliated with the company.
25. Creating, forwarding, or exchanging SPAM, chain letters, solicitations, or advertising.
26. Creating, storing, or exchanging e-mail that violates material protected under copyright laws.
27. Distributing school's or institution's data without proper authorization.
28. Altering a message from another user without their permission
29. Opening e-mail without performing a virus scan.
30. Improperly using someone else's e-mail account as your own without their permission

3.3 User Responsibilities

Al users who use the Internet or Internet e-mail shall:

1. Ensure that all communications are for work reasons and that they do not interfere with his/her education and or productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the user's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable laws, regulations and policies including laws, regulations and polices dealing with security and confidentiality of institutional records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of nonpublic information. If it is necessary to transmit nonpublic information, users are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

3.4 P2P

Peer-to-peer (P2P) file networking technology enables one computer to communicate directly with another computer that has the P2P application, bypassing the organization's centralized server in the process. Each computer on this P2P network can act as a server and publish information, to be shared by any other computer on the network. Kazaa, the well-known file-sharing network, is an example of P2P technology at work.

Running P2P programs on company PCs or through company servers opens the organization to three primary risks:

1. Bandwidth Waste: P2P file trading networks offer one of the most convenient ways to distribute large digital files including video, streaming audio and MP3 files. Unless files

are being transmitted for legitimate business purposes, valuable network bandwidth and hard drive space are wasted on frivolous content;

2. Security Breaches: P2P use can open a direct pipeline from hackers into your enterprise. File trading works by exposing folders and directories to other network users, effectively opening up the computer to the world. It's also fairly easy to disguise a Trojan horse, a virus, or other malicious code as a harmless file type, fooling a user into downloading it directly to their hard drive. The result could be extensive damage to your organization's computer system;
3. Legal and Copyright Concerns: Record labels, film studios, software vendors and other copyright holders have been aggressive in prosecuting copyright infringement perpetrated through P2P.

3.4.1 P2P use

The use of P2P programs leads to significant risks to IT equipment, networks, information systems, and institutions and there its use is strictly prohibited to all users.