GOVERNMENT OF SAMOA

MINISTRY OF HEALTH INTERNET AND SOCIAL MEDIA POLICY 2020

OCTOBER 2020

Table of Contents

OVERVIEW 2

PURPOSE 2

SCOPE 2

OBJECTIVE: 2

POLICY 2

OVERVIEW

Employees have access to e-mail and internet accounts to conduct work requirements for the Government of Samoa through the Ministry of Health. The use of MoH facilities and equipment shall be conducted in a way which keeps the integrity and professionalism of the MoH as well as the integrity of the MoH information technology and communications facilities and equipment.

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include social web-applications and networking, blogs, wikis, micro blogs, message boards, chats, and other sites and services that permit users to share information with others in a contemporaneous manner.

PURPOSE

The rapidly growing trend of user-generated web content such as blogging, social web applications and networking, are important arenas for communications, employee engagement andlearning. This policy provides practical guidelines to employees when participating in online social media activities and is in no way intended to inhibit or prevent employees from expressing their personal views when engaging in social media for personal use.

SCOPE

This policy applies to employees, clinicians and clinical professionals accessing Ministry of Health facilities and sites (i.e. visiting specialists, private practitioners, volunteers), non-employee assistants/students, vendors, contract personnel and individuals otherwise obligated to follow MOH policies and procedures.

OBJECTIVE:

The Ministry of Health (MOH) recognizes the importance and benefit of having access to Internet in efficiently and effectively obtaining valuable information for conducting workplace day to day activities. However, due to budget constraints internet access is granted to users provided that the manager of the respective division justifies that usage is solely for the purpose of performing their jobs and professional roles.

This policy outlines MOH' guidelines for acceptable use of its internet services and this policy must be followed in conjunction with other MOH policies governing appropriate workplace conduct and behavior. Internet accessed through any Information and Communication Technology (ICT) device or resource belonging to MOH is a property of MOH and therefore MOH has the right to monitor all employee usage and content of their internet usage. All users are expected to be familiar with and comply with this policy. Non-compliance could result in disciplinary action which may include revocation of internet up to and/or including termination.

POLICY

1. INTERNET ACCESS REQUEST and APPROVAL

Internet usage is a privilege provided only on an as-needed basis to support MOH activities and perform the user's professional duties.

1.1 Usage Request

Users requiring access to internet must first read this Internet Policy plus other relevant policies before completing and signing the *ITA1 Form*. Signing this form indicates the user has read, understood and agrees to comply with the policies. This request must then be justified by the relevant divisional leader and endorsed by the A.CEO ITC

1.2 Usage Approval

The request is finally approved or disapproved by the Director General (or Deputy Director General in the absence of the Director General). The form will then be returned to the ITC Division for actioning the approved requests and notify user when actioned.

1.3 Usage Disapproval

The request for internet access will be denied if the justification for internet access is not satisfactory.

1.4 Blocking Sites

Specific sites will have been blocked for purposes relating to security, networkperformance and confidentiality of MoH Information and to prevent access to sites that contain illegal content. The list, nature and range of blocked sites is determined by the ITC Division, having consulted with Management and technical staff.

1.5 Removal of Internet Access

1.5.1 Access to the internet will be discontinued upon termination of an employee, completion of contract, end of service of temporary employee or disciplinary action resulting from violation of this policy.

1.5.2 In the case whereby an employee has been transferred to another sector within MOH or a change in the users' job functions is done the original internet access password will be discontinued and a new request for access must be submitted for approval.

2. INTERNET PASSWORD

2.1. Not everyone in MOH has the privilege of accessing the internet and those who are authorized to access the internet must guard and not share their passwords with others.

2.2. Do not use your own name, names of family members or birthdates as passwords as these are very easily guessed.

2.3. Disclosing of passwords for use by others is considered a violation of this policy and the user may be subject to disciplinary action that may include removal of internet access.

2.4. Everyone is advised to also read and familiarize themselves with the Samoa Crimes Act 2013, where it also highlights and emphasizes an imprisonment term of not more than 7 years once proved of unauthorized access to a system.

3. ACCEPTABLE INTERNET USAGE

Access to internet is granted for the sole purpose of supporting activities necessary in performing MOH job functions. Such activities may include but not limited to

- Communication between employees and its stakeholders for business purposes.
- Employee educational and professional development.
- IT technical support for downloading software upgrades and patches.
- Conducting research for MOH job related activities.
- Obtaining health service information.

4. UNACCEPTABLE INTERNET USAGE

Strictly prohibited activities include, but are not limited to:

4.1 The acquisition, storage and dissemination of data which is illegal, pornographic or which negatively depicts race, sex or creed is specifically prohibited.

4.2 MOH also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

4.3 Deliberate pointing or hyper-linking of the MOH website to other internet/www sites whose contents may be inconsistent with or in violation of the policies of the Ministry.

4.4 Use, transmission, duplication or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets or patent rights of any person, group or organization. Users are to assume that all materials on the internet are copyright and/or patented unless specific notices state otherwise.

4.5 Transmission of any proprietary, confidential or otherwise sensitive information without the proper controls.

4.6 Creation, posting, transmission or voluntary receipt of any unlawful offensive, libelous, threatening, harassing material including, but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion or political beliefs.

4.7 Accessing sites that involve:

4.7.1 Any form of gambling is strictly prohibited.

4.7.2 auctioning / buying / selling

4.7.3 dating

4.7.4 Playing of any online games.

4.7.5 grooming

4.8 Unauthorized downloading of any shareware or spyware programs or files for use without advance authorization from the IT department and the user's manager.

4.9 Participation in any online contest or promotion.

4.10 Forwarding of chain letters.

4.11 Acceptance of promotional gifts.

5. PERSONAL USAGE

5.1 All users must follow the corporate principles regarding resource usage and exercise good judgment when using the Internet. Access to the internet by personnel that is inconsistent with corporate needs of MOH results in the misuse of resources.

5.2 Usage of MOH computer resources to access the internet for personal purposes without approval may be considered cause for disciplinary action.

5.3 All users must be aware that the Ministry network creates a log of all access activities reflecting the types of websites visited.

5.4 Users who choose to store or transmit personal information such as bank pin numbers or related details as well as credit card numbers on MOH devices or network do so at their own risk. MOH is not responsible for any loss of information, such as information stored online and accessed through MOH ICT resources, or any consequential loss of personal property due to such processes.

5.5 Any ordering (shopping) of items or services on the internet for personal usage is strictly prohibited.

6. DOWNLOADS

6.1 Downloads of any software other than what is already pre-installed on user computer and devices is strictly forbidden. The ITCDivision must be consulted if additional software needs to be installed and ITCDivision will act accordingly.

6.2 The download of any games, movies or non-work related materials are strictly forbidden.

7. UPLOADS

Upload of any MOH materials or information or any information that may cause defamation to MOH and/or its services without authorization is strictly prohibited

8. SOFTWARE LICENSE

MOH strongly supports strict adherence to software vendor's license agreements. When at work, or when MOH computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden.

Similarly, reproduction of materials available over the internet must be done only with written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of materials from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of fair use is in keeping with international copyright laws.

9. MONITORING of INTERNET ACCESS AND USAGE

All users of MOH internet services should consider their internet activities periodically monitored and limit their activities accordingly.

Management of MOH reserves the right to examine E-mail, personal file-directories, web access and other information stored on Ministry computers, at any time and without prior notice. This examination ensures compliance with internal policies and assists with the management of Ministry information systems.

10. MAINTAING CORPORATE IMAGE

10.1. When using Ministry resources to access and use the internet, individuals must realize that they represent the corporation. Whenever an employee states an affiliation to MOH**,** they must also clearly indicate that"*the opinions expressed are my own and not necessarily those of MOH*"**.**

10.2. Individuals must not place corporate material (example: internal memos, press releases, government confidential documents, product or usage information, etc.) that is not already made public on any mailing list, public news group, social media, or such service. Any posting of materials must be approved by management and posting will be done by an authorized individual

10.3. If an individual is contacted by a blogger, online journalist or media representative about any business of the MOH, he/she must notify their Manager or General Manager before responding.

11. SOCIAL MEDIA

Employees may at their own accord be members of social networking sites or may engage in other online chat groups, blogs, and other sites. Employees are not allowed to identifying themselves as employees of the MoH when posting comments on the internet or on other on-line services. Messages and posts sent via the MoH ICT facilities and equipment will be easilyidentifiable as being from an employee of the MoH; hence participation in internet newsgroups and the like using the MoH equipment or facilities is therefore prohibited.

Employees must understand and agree that, when engaging in social media activities, they must comply at all times with MoH workplace obligations, including but not limited to obligations in regard to loyalty and confidentiality, as well as with respect to all human rights policies, guidelines and applicable legislation.

Using Social Media for Work

Employees shall not disclose confidential or proprietary information or similar information of thirdparties, including but not limited to stakeholders who have shared such information with the MoH. The MoH intellectual property, trademarks, and copyrights shall not beused in any manner without the approval of the MoH.

The MoH reminds all employees that the Code of Conduct and Code of Ethics must be respected whileparticipating in blogs, on-line discussion forums or any other social media activities. All

employees are to represent the MoH in a professional manner as would be expected in anyother public forum or medium, and should exercise discretion, thoughtfulness and respect for colleagues.

Employees must ensure that they have all the facts before posting information to avoid having to post acorrection or a retraction. Should an error occur, it should be corrected quickly and visibly.Employees are not permitted to use the MoH social media channels for which they havelogin credentials for self-promotion or the promotion of their own personal business or creative projects.

Personal Use of Social Media
The following is a non-exhaustive list of requirements when employees are using social media for non-work purposes:

- Do not share photos or personal information about the Ministry, Executive Management, Colleagues oranyone else with whom the employee has come into contact with in the course of employment with the MoH;
- Do not share any confidential information of any kind, including patients' information; computer passwords, security information, ID information, or any other information obtained in the course ofemployment.

Employers, including the ITC Division, have the ability and the right to monitor social media sites.Employees who post information that adversely impacts the interests of the MoH, breaches confidentiality or irreparably undermines their employment relationship will be disciplined up toand including termination of employment.

Individuals are legally liable for what they post on their own site(s) and on the sites of others. Individualbloggers can be held liable for commentary deemed to be proprietary, copyrighted, defamatory, libellousor obscene (as defined by the courts).

Personal Devices

An employee may use their personal device(s) in the performance of their job duties on the understandingthat the use of a personal device in connection with the MoH facilities is a privilege grantedto employees through approval of management. Employees are not permitted to use personal deviceswithout having obtained the advance written permission of the Director General or delegate. The MoH reserves the right to revoke the privilege at any time and for any reason. Users of personal devices for MoH related work must agree to all terms and conditions in this Policy to bepermitted access to the MoH networks. The MoH reserves the right to disable ordisconnect some or all of its remote services without prior notification to employees.

Users of personal devices are responsible for keeping their devices current and this includes, but is notlimited to, ensuring the device has all recent security, software and firmware updates. Any device whichis used to access MoH systems and/or networks must be equipped with a password lock. Only ICT employees will be permitted to access our data on personal devices. Should the employeelose or report their personal device stolen, the ICT Division must be notified as soon as possible toprevent unauthorized access to the network from the missing device. Employees are responsible fornotifying their mobile carrier immediately upon loss of a device.

As a condition of using personal devices for MoH work, employees consent that the ICT Division may intercept, access, retrieve, read, disclose, and use any telephone or voice mailcommunications and/or computer systems activity, including Internet access and electronic mail, on apersonal device, for the same purposes as set out in section (vii) above.

In using their personal device to fulfil job functions, the employee recognizes that they have a diminishedexpectation of privacy with regards to their personal device.

11.1. Unless approved by the MOH management, your social media name, URL, profile photo and such should not utilize the MOH logo or proprietary graphics.

11.2. Whatever you post on a social media site instantly becomes public. Regardless of your privacy settings, your content can easily be made available to those outside of your preference settings. You are entirely responsible for what you post online.

11.3. Social media content must comply with all of our hospital policies including, but not limited to our Code of Conduct, communication, confidentiality, discrimination and harassment policies.

11.3.1. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees, or otherwise adversely affects clients, patients, vendors, suppliers, or people who work on behalf of the Ministry's legitimate business interests, may result in disciplinary action up to and including termination.

11.4. Employees are advised to always be courteous to fellow employees, clients, patients, vendors, and suppliers. You are more likely to resolve work problems by speaking directly with your co-workers or supervisor(s) than by posting complaints on social media. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that are malicious, obscene, threatening or intimidating, that disparage employees, clients, customers, vendors or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation, or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or Ministry policy.

11.5. Write in the first person. Where your connection to MOH is apparent, make it clear that you are speaking for yourself and not on behalf of MOH unless authorized to do so. In those circumstances, you should include a disclaimer such as: "The views expressed on this [blog; website; posting] are my own and do not reflect the views of my employer."

11.6. Individuals must not share or disclose confidential or proprietary information about MOH.

11.6.1. Individuals are responsible for any publicly viewable intentionally false statements that damage the organization or the service's reputation.

11.7. Individuals may not use or disclose any patient identifiable information of any kind. Posting of photos, video and sound recordings of patients being cared for in MOH, without their prior written consent are strictly prohibited.

11.7.1. Even if the patient is not identified by name within the information at issue, if there is reasonable basis to believe that the person could still be identified from that information, then its use or disclosure could constitute a violation of this policy.

11.7.2. Any online activity regarding patients cared for by MOH that may compromise a patient's personal dignity or otherwise make them question the confidentiality of the services provided by any of its facilities are prohibited.

11.8. Staff must not cite or reference business associates or co-workers without their approval.

11.9. Staff members are prohibited from using their MOH.gov.ws email address to register on blogs, social networks or other forms of social media.

11.10. Staff in management/supervisory roles are discouraged from initiating "friend" requests with employees they manage. Managers/supervisors may accept friend requests if initiated by the employee, and if the manager/supervisor does not believe it will negatively impact the work relationship.

11.11. "Friending" of patients on social media websites are strongly discouraged. Staff in patient care roles generally should not initiate or accept friend requests.

12. POLICY COMPLIANCE

The IT Unit will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits and feedbacks to the policy from the users.

Any exception to this policy must be approved by the IT Unit in advance.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Additionally, MOH may at its discretion seek legal remedies for damages incurred as a result of any violation. MOH may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the internet via MOH network is approved, the potential user is required to read this Internet Usage Policy and sign the acknowledgment section of the *ICT Access Form*. The completed form must then be turned in and will be kept on file at the IT department. For any further questions regarding the Internet Usage Policy, contact the IT department.

Violations of this Policy

Any violations of this Policy, in whole or in part, may result in disciplinary action which may include, but not be limited to, termination of employment or contract and/or such other legal actions as may be warranted in the circumstances.

13. RELATED POLICIES and REGULATIONS

Samoa MOH Act 2014
Samoa Crimes Act 2013
Samoa Copyright Act1998