	POLICY Number: 7311-25-002 Title: Internet Acceptable Use
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-003, 7311-25-004 Date Approved: October 10, 2000 Date Revised: May 13, 2013 Date Effective: May 30, 2013 Date Reaffirmed: Scope: SHR & Affiliates

Overview

The Internet is a global network of networks that provides access to a myriad of reference sources and information systems. Internet access provided by SHR is a clinical, business, and technical resource that competes with other critical applications for limited internal and external network bandwidth. As such, it is important that SHR Users use this Internet access responsibly, for SHR business related purposes, and in a manner that adheres to SHR's Vision, Mission, Values, Goals, workplace philosophy statements, policies and procedures.

Definitions

Internet means an open and public network, encompassing any World Wide Web page that is accessible by any Internet user, including SHR Users. Internet resources include, but are not limited to: web sites, email, file transfer protocol, blogs, or news and discussion groups.

SHR Intranet (InfoNet) means SHR's internal web site, where information is to be accessed and shared by SHR Users only.

SHR User means a person with an active SHR User Account that allows access to the SHR computer network. A SHR User may include SHR employees, affiliate employees, physicians, other health care professionals, students, contractors, vendors and any other person who has been approved for a SHR User Account.

SHR User Account means a personal account consisting of an Active Directory username and a password that is granted user access privileges, as specified on the *SHR User Account Application Form*. Privileges may include access to shared files, email and/or systems/applications.

1. PURPOSE

The purpose of this policy is to establish acceptable and unacceptable use of SHR Internet resources.

2. PRINCIPLES

2.1 Internet access is a privilege, not a right.

2.2 Appropriate use of the Internet protects the integrity, confidentiality and availability of SHR computing resources.

3. POLICY

3.1 Access

3.1.1 The authority to approve and remove/deny Internet access rests with a SHR User's Manager. It shall be at a Manager's discretion to restrict Internet use, and deny or remove Internet access for SHR Users for whom they are responsible, at any time.

3.1.2 Saskatoon Health Region (SHR) will provide access to the Internet to SHR Users through the department of Information Technology Services (ITS).

3.1.3 ITS reserves the right to block access to web sites that do not adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements and policies.

3.2 Conduct

3.2.1 SHR Users of the Internet must adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements, policies and procedures.

3.2.2 Internet access provided by SHR shall be used for SHR related business use and communication.

3.2.3 Limited personal use of the Internet by SHR Users is acceptable, provided it occurs only on the employee's own time and is in compliance with this policy.

3.2.4 SHR Users will use the Internet for purposes that are respectful of others, legal and ethical. Users will not access Internet sites that are inappropriate to job functions or do not adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements and policies.

3.2.5 SHR Users accessing the Internet must strictly adhere to all laws, copyright laws, codes of conduct, the Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP), the Health Information Protection Act (HIPA), the Personal Information Protection and Electronics Document Act, (PIPEDA) and any other applicable federal and/or provincial legislation on privacy and confidentiality.

3.2.6 *Exercise* caution *when emailing Personal Health Information (PHI), as this is only allowed under very specific circumstances.* If you feel you must email PHI, refer to SHR's policy Emailing Personal Health Information for specific rules and restrictions.

3.3 Acceptable Use

SHR Users are encouraged to use the Internet to further the Vision, Mission, Values, Goals, and workplace philosophy statements of SHR.

3.3.1 The types of activities that are encouraged include:

- Communication with fellow employees, affiliated agencies, organizations, and other health regions within the context of an individual's assigned responsibilities.
- Acquisition or sharing of information necessary for or related to the performance of an individual's assigned responsibilities. (See SHR's Privacy and Confidentiality policy.)
- Participation in educational or professional development activities.

3.3.2 Corporate Image

- In all communications, SHR users will ensure that they are representing the Region in a positive manner by identifying themselves honestly, accurately and completely while maintaining SHR's integrity and credibility.
- SHR Users will ensure that external communication is not inflammatory, harassing, defamatory, disruptive to other companies, organizations, and/or individuals, and will not compromise SHR's reputation or image.
- Only authorized SHR staff will communicate on behalf of SHR to any on-line media or public news group.

3.4 Unacceptable Use

Unacceptable use of the Internet includes, but is not limited to the following:

3.4.1 Illegal or unlawful purposes, such as copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. hacking or intentional spreading of computer viruses).

3.4.2 Accessing, distributing, or displaying objectionable material, including but not limited to:

- Obscene or pornographic material;
- Hate propaganda or discriminatory material;
- Defamatory and libellous material; and
- Sexually harassing material.

3.4.3 Posting any client, patient or resident information on the Internet.

3.4.4 'Spamming' (sending or forwarding unwanted information to any group of people) or other forms of mass unsolicited mailings, including the dissemination of

chain letters or political campaigning.

3.4.5 Access by non-SHR Users to SHR resources or network facilities.

3.4.6 Competitive commercial activity unless pre-approved by SHR.

3.4.7 Forwarding frivolous emails, such as, jokes, trivia, stories, animated greeting cards, promotional material, video/music media clips, and personal photos.

3.4.8 Viewing, copying, altering, or destroying data, software, documentation, or data communications belonging to SHR or another individual without authorized permission.

3.4.9 Use of the internet for streaming or downloading audio or video, such as online radio, news clips, movies, etc., unless for business purposes.

3.4.10 Downloading software or files (see Section 3.7 Downloading from the Internet).

3.4.11 For additional guidelines, please refer to SHR's Social Media policy.

3.5 Privacy and Confidentiality

3.5.1 All information stored on computer equipment or accessed via the SHR network is the property of SHR.

3.5.2 SHR Users should have no expectation of privacy for any information posted to the Internet or obtained from the Internet that is stored on SHR computer equipment.

3.5.3 LA FOIP allows the general public the right to request access to any administrative records in the custody of SHR through a Freedom of Information Request.

3.5.4 SHR retains the right to copyright any material posted to any forum, news group, chat group or web page by any SHR User in the course of his/her duties or while representing SHR or using SHR resources.

3.5.5 If SHR discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, Internet activity records may be retrieved and used to investigate the activity in accordance with due process.

3.5.6 SHR reserves the right to access, review, retrieve or copy all Internet activity for any SHR business purpose and to disclose these records to any appropriate party including courts and law enforcement authorities.

3.6 Security

3.6.1 SHR Users and all employees of SHR must report unacceptable Internet use immediately to their Manager.

3.6.2 SHR Users will strictly adhere to all laws, copyright laws, codes of conduct, SHR privacy and IT policies, LA FOIP, HIPA, PIPEDA and any other applicable federal and/or provincial legislation on privacy and confidentiality including the collection, use, storage and disclosure of personal health information.

3.6.3 SHR Users shall be responsible for any activity carried out under their user account. (See the SHR User Account Policy.)

3.6.4 SHR Users are solely responsible for any material that they access and disseminate through the Internet.

3.6.5 SHR assumes no liability for any direct or indirect damages arising from a SHR User's connection to the Internet. SHR is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems.

3.6.6 ITS reserves the right to block access to web sites that do not adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements and policies.

3.7 Downloading from the Internet

3.7.1 Downloading executable software is strictly prohibited without prior permission from ITS. Examples of executable files are those files ending in .exe or .vbs.

3.7.2 Downloading any executable software may cause activation of harmful computer viruses that may result in computer damage.

3.7.3 Any software or files downloaded via the Internet onto SHR computer equipment will become the property of SHR. Any such files or software will be used only in ways that are consistent with their licenses or copyrights.

3.7.4 Downloading of large files is prohibited unless required for SHR related business.

3.8 Monitoring

SHR has the right to monitor and use monitoring tools, on all Internet activity occurring on the SHR network. If activities are discovered that do not comply with applicable law or SHR policy, Internet usage records retrieved may be used to document the wrongful content in accordance with due process.

3.8.1 ITS will monitor Internet usage by:

- Recording for every user, each web site visit, chat, news group and file transfer into and out of the internal network.
- Using software tools to identify socially inappropriate or sexually explicit Internet sites.
- Reporting unacceptable use or illegal activity to an ITS Manager, who is responsible for contacting the appropriate law enforcement agency and/or the Care Group/Service Department's Manager. In the event that law enforcement becomes involved, SHR's Director of Risk Management shall be notified.

3.9 Investigations

3.9.1 SHR will investigate:

- Unacceptable use or illegal activity on the Internet that has been reported or detected.
- Requests by a Manager to view the Internet activity of a SHR User for whom they are responsible. Such requests must be approved by an ITS Manager, who will validate that the request's purpose is consistent with the goal of detecting possible violations of this policy.

3.9.2 All investigative findings and Internet usage reports will be sent to an ITS Manager, who will follow up as required on all investigative findings, Internet usage reports, and reports of unacceptable or illegal activity with the appropriate law enforcement agency and/or the Care Group/Service Department's Manager. In the event that law enforcement becomes involved, SHR's Director of Risk Management shall be notified.

3.9.3 ITS will not investigate unsubstantiated (spurious 'fishing expedition') requests by a Manager to view Internet activity.

3.9.4 In confirmed cases of unacceptable use by an SHR User, it is the Manager's responsibility to take measures in accordance with SHR human resources procedures.

3.9.5 SHR and SHR Users will cooperate fully with external investigations where the investigation is related to a SHR User using SHR resources inappropriately.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users shall:

4.1.1 Use Internet access provided by SHR for SHR related business use and communication in compliance with this policy and those indicated in the Reference section below.

4.1.2 Report unacceptable Internet use immediately to their Manager.

4.1.3 Cooperate fully with external investigations where the investigation is related to a SHR User (including themselves) using SHR resources inappropriately.

4.2 Managers shall:

4.2.1 At their discretion, restrict, deny or remove Internet access for SHR Users for whom they are responsible if these users do not utilize Internet access in accordance with the principles and provisions of this policy.

4.2.2 Cooperate fully with external investigations where the investigation is related to a SHR User using/potentially using SHR resources inappropriately.

4.2.3 In confirmed cases of unacceptable use by an SHR User, take measures in accordance with SHR human resources procedures.

4.3 ITS Infrastructure shall:

4.3.1 Reserve the right to block access to web sites that do not adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements and policies.

4.3.2 Retrieve and use Internet activity records to investigate further if user or system activities are discovered or detected that do not comply with applicable laws or this policy.

4.3.3 Reserve the right to access, review, retrieve or copy all Internet activity for any SHR business purpose and to disclose these records to any appropriate party including courts and law enforcement authorities.

4.3.4 Send all investigative findings, Internet usage reports, and reports of unacceptable use or illegal activity to IT Security.

4.4 IT Security shall:

4.4.1 Investigate unacceptable use or illegal activity that has been reported or detected.

4.4.2 Cooperate fully with external investigations where the investigation is related to a SHR User using SHR resources inappropriately.

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

6. NON-COMPLIANCE/BREACH

Non-compliance with this policy will result in a review of the incident. A review for non-compliance may result in disciplinary action, up to and including termination of employment and/or privileges with SHR.

7. REFERENCES

Respect and Dignity

Privacy and Confidentiality

Information Classification, Labeling and Handling

IT Security

SHR User Account Policy

Email Acceptable Use

Emailing Personal Health Information

Social Media