

	POLICIES & PROCEDURES Number: 7311-25-002 Title: INTERNET ACCEPTABLE USE POLICY
Authorization <input type="checkbox"/> Board of Directors <input type="checkbox"/> Senior Leadership Team <input checked="" type="checkbox"/> Vice President	Source: Information Technology Services (ITS) Cross Index: Date Approved: October 10, 2000 Date Reaffirmed: Date Revised: Date Effective: October 9, 2007 Scope: Saskatoon Health Region Users

DEFINITIONS:

Internet: an open and public network, encompassing any World Wide Web page that is accessible by any Internet user, including SHR Users.

SHR Intranet (InfoNet): the SHR internal web site that allows information to be accessed and shared by SHR users only.

SHR User: 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 an SHR User Account.

SHR User Account: 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. POLICY

- 1.1 Saskatoon Health Region (SHR) will provide access to the Internet to all SHR Users through the department of Information Technology Services (ITS).
- 1.2 SHR Users of the Internet must adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements, policies and procedures.
- 1.3 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.

- 1.4 Internet access provided by SHR shall be used for SHR related business use and communication.
- 1.5 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.

2. PURPOSE

- 2.1 To communicate acceptable and unacceptable use of SHR Internet resources to SHR users. Internet resources include, but are not limited to: web sites, email, file transfer protocol, blogs, or news and discussion groups.
- 2.2 To ensure the Internet is used efficiently and effectively to protect the integrity, confidentiality and availability of SHR computing resources.

3. PROCEDURE

3.1 Access

- ITS provides Internet access to all SHR User Accounts at SHR.
- A Manager can request to have Internet access removed from a SHR User Account, for SHR Users for whom they are responsible, by contacting ITS Security.

3.2 Acceptable Use

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

The types of activities that are encouraged include:

- Communication with fellow employees, affiliated agencies, organizations, other health regions, etc. 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.
- Participation in educational or professional development activities.

3.2.1 Principles

- SHR Users will abide by Regional policies, especially those policies that deal with privacy and confidentiality, misuse of Regional resources, issues surrounding respect and dignity, information and data security, communication, and SHR User Accounts.

- SHR Users will use the Internet for purposes that are respectful of others, legal and ethical.
- Internet access is a privilege, not a right.
- 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.
- 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.

3.2.2 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.

3.3 Unacceptable Use

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

- Illegal or unlawful purposes, such as copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Posting any identifiable client, patient or resident health information on the Internet.
- '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.
- Access by non-SHR Users to SHR resources or network facilities.
- Competitive commercial activity unless pre-approved by SHR.
- Forwarding frivolous emails, such as, jokes, trivia, stories, animated greeting cards, promotional material, video/music media clips, and personal photos.

- Viewing, copying, altering, or destroying data, software, documentation, or data communications belonging to SHR or another individual without authorized permission.
- Use of the internet for streaming or downloading audio or video, such as online radio, news clips, movies, etc., unless for business purposes.
- Downloading software or files (see Section 3.6 Downloading from the Internet).

3.4 Privacy and Confidentiality

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

3.5 Security

- SHR Users and all employees of SHR must report unacceptable Internet use immediately to their Manager.
- SHR users will strictly adhere to all laws, copyright laws, codes of conduct, ITS Data Access Rules and Regulations, 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.
- SHR Users shall be responsible for any activity carried out under their user account. (See Saskatoon Health Region User Account Policy);
- SHR Users are solely responsible for any material that they access and disseminate through the Internet.
- 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.

- 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.

3.6 Downloading from the Internet

- Downloading executable software is strictly prohibited without prior permission from ITS. Examples of executable files are those files ending in .exe or .vbs.
- Downloading any executable software may cause activation of harmful computer viruses that may result in computer damage.
- 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.
- Downloading of large files is prohibited unless required for SHR related business.

3.7 Failure to Comply

Violations of this policy will be adjudicated according to established SHR policies and procedures.

3.7.1 Sanctions for unacceptable use of the Internet may include, but are not limited to, one or more of the following:

- Temporary or permanent loss of privileges for access to some or all computing and networking resources and facilities.
- Disciplinary action by the manager, in consultation with Labour Relations, according to applicable SHR policies, up to and including termination of employment.
- Legal action according to applicable federal and provincial laws and contractual agreements.

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. Users will not access sexually explicit Internet sites or Internet sites that are inappropriate to job functions or do not adhere to SHR's Vision, Mission, Values, Goals, workplace philosophy statements and policies.
- 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.

3.9 Internet 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 an 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 with the appropriate law enforcement agency and/or the Care Group/Service Department's Manager.

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