	POLICY Number: 7311-25-001 Title: EMAIL ACCEPTABLE USE
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-005 Date Approved: November 18, 2011 Date Revised: March 4, 2015 Date Effective: March 10, 2015 Date Reaffirmed: Scope: SHR & Affiliates

OVERVIEW

This policy covers email acceptable use pertaining to general day to day use for SHR business. It is not intended nor does it include details on the use of the email system for sending confidential/personal health information external to the SHR network. Please refer to the SHR Policy: *Emailing Personal Health Information* or contact the Privacy and Access Department.

DEFINITIONS

External Email Address means any non-SHR email address where messages are sent outside the secure SHR network. Such addresses include, but are not limited to any address in the global address book that is not a Saskatoon Health Region address and email services provided by an external provider (e.g. Gmail, Shaw, SaskTel, Yahoo, Hotmail, etc.).

Saskatoon Health Region (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 an SHR User Account.

Saskatoon Health Region (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 the SHR Email System for all SHR User Account holders.

2. PRINCIPLES

2.1 Email is a critical mechanism for business communication.

2.2 The SHR Email System is intended to be used efficiently and effectively while protecting the integrity, confidentiality and availability of regional computing resources.

3. POLICY

3.1 Access

SHR Information Technology Services (ITS) shall control access to the SHR Email System through the SHR User Account application process.

3.2 Conduct

3.2.1 SHR Users shall:

- Use the Email system for purposes that are respectful of others. Access to the Email system is a privilege, not a right.
- In all communications, ensure that they are representing SHR in a positive manner by identifying themselves honestly, accurately and completely while maintaining SHR's integrity and credibility.
- Ensure that communication does not compromise SHR's reputation or image, and is not inflammatory, harassing, defamatory, or disruptive to other companies, organizations, and/or individuals.

3.3 Distribution of Email Messages to All SHR Users (Mass Email)

3.3.1 **Access and Authorized Users**

Authorized use of the 'All SHR Users' distribution option shall be restricted due to the stress that such email places on the SHR network. Use of this option shall be limited to timely or urgent communication only.

There are few email messages that are appropriate for mass distribution. Authorized use of the '**All SKTNHR Email Users'** distribution list available in the global address book shall be limited to:

- Senior Leadership Team (SLT);
- Emergency Preparedness Director and Site Leaders;
- Administrative Assistants for the above two groups;
- Designated Information Technology Services (ITS) staff as determined by the Director, ITS;
- All Communications department staff and associated email accounts such as The Region Reporter, Region Weekly, etc.)

3.3.2 **Distribution**

Email messages to all SHR Users must be distributed in accordance to the Mass Email Distribution Guidelines.

3.4 Acceptable Use of Email

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 or related to the performance of an individual's assigned responsibilities.
- Participation in educational or professional development activities.

3.4.1 **Personal Use**

- Limited personal use of the SHR Email System by SHR Users is acceptable, provided it is brief, occasional, on the employee's own time, does not involve the receipt or transmission of large file attachments, and is in compliance with this policy.
- A Manager can deny personal use of email by staff in their department, at their discretion.

3.4.2 Sending Personal Health Information (PHI) (see the SHR Policy: *Emailing Personal Health Information*).

3.4.3 Only the SHR Communications Department shall communicate on behalf of SHR to any on-line media or public news group.

3.5 Unacceptable Use of Email

The SHR Email System and Services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems or interfere with others use of the SHR Email System and Services. Unacceptable use of the SHR Email System and Services includes, but is not limited to, the following:
SHR Users shall not:

- Allow another person to use their user account to access their SHR email mailbox, or other mailboxes for which they have access.
- Attach a scanned document containing their signature, unless it is for the purpose of conducting SHR business with another SHR business unit, vendor, etc. Recipients of emails with such attachments should save the attachment and delete the email. Emails should not be forwarded on to others who do not require the attachment that contains a signature. Users may wish to include a warning with a request not to forward and to delete the email when no longer required.
- Store personal email in their SHR mailbox.
- Use internal distribution lists to send non-SHR business related material.
- Conduct SHR business on a non-SHR email account or forward SHR e- mail from your SHR mailbox to a non-SHR email account, such as a personal email account (e.g. Hotmail, Yahoo, Shaw, SaskTel, etc.). Sending SHR email over the unsecure public internet is a security risk as email could be intercepted, copied or altered. SHR Users should use SHR webmail to remotely access their SHR mailbox.
- Send large email attachments that may result in an 'undeliverable' e- mail message. The email system limits the size of large email attachments due to limited system capacity. If in doubt about the types or size of files that may be sent, SHR Users should consult the ITS Service Desk.

- Open email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Force entry into another user's SHR User Account to access their email or use their email address without the account holder's or the account holder's manager's permission.
- Send or forward 'Spam' (i.e. sending unsolicited or unwanted information to any group of people) or other forms of mass unsolicited mailings, including the dissemination of chain letters or political campaigning.
- Allow non-SHR Users access to SHR resources or network facilities.
- Use SHR email for commercial activity for personal gain.
- Use the email system for illegal or unlawful purposes, such as copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, gambling, soliciting for pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

3.6 Privacy

- Use of the SHR Email System by an SHR User shall constitute an irrevocable consent to the monitoring and disclosure of system use and data, with no expectation of privacy.
- SHR reserves the right to access, review or copy all email messages for any SHR business purpose and to disclose them to any appropriate party including courts and law enforcement authorities.
- The email system and all email stored on it, is the property of SHR. This includes all email transmitted, received and stored on individual SHR User Accounts.
- SHR Users shall strictly adhere to all laws, copyright laws, regulations, *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), *The Health Information Protection Act* (HIPA), *The Personal Information Protection and Electronic Documents Act* (PIPEDA) and any other applicable federal and/or provincial legislation.
- LA FOIP allows the general public the right to request access to any administrative records (including email) in the custody of SHR through a Freedom of Information request.
- The SHR Email system does not use encryption on any type of email message being sent or received.
- All email messages sent outside of the SHR become the property of the receiver and SHR no longer retains control over who might view those messages or who they might be forwarded to. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" or "Reply to All" command during email correspondence.
- SHR is under no obligation to store or forward the contents of a SHR User's email mailbox upon termination.
- SHR will not actively read end-user email without just cause, but email messages may be inadvertently read by IT staff during the normal course of managing the SHR Email System.
- Backup copies of email messages may exist, despite end-user deletion, for record retention purposes.

- SHR assumes no liability for any direct or indirect damages arising from the use of the SHR Email System. Saskatoon Health Region is not responsible for the accuracy of information received or sent on the SHR Email System and only facilitates the access and dissemination of information through its systems.

3.7 Signatures

SHR Users shall use email signatures that conform to the SHR email signature standards (see the Email Signature Guidelines). Unacceptable email signatures include, but are not limited to, the following:

- Attaching a scanned copy of their handwritten signature
- Use of background images or signature attachments (e.g. icons, animated GIFs, etc.)

3.8 Disclaimer

The following disclaimer shall be used by SHR Users on all email messages sent outside the SHR network. This includes 'New', `Reply', `Reply To All', and `Forward'. The disclaimer can be added to a SHR User's email 'signature' (refer to ITS InfoNet site, "Self Help" section for Email for how to add the disclaimer).

This email message may contain confidential and/or privileged information. It is intended only for the addressee(s). Any unauthorized disclosure is strictly prohibited. If you are not a named addressee you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. Email transmissions cannot be guaranteed to be secure or error free as information could be monitored, intercepted, corrupted, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept any liability for errors or omissions in the contents of this message or any damages that arise as a result of email transmissions.

This disclaimer has been approved by the Saskatchewan Office of the Information and Privacy Commissioner and adopted for use by SHR.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users

4.1.1 New applicants must read and sign a copy of the SHR Confidentiality Agreement.

4.1.2 Read and comply with this policy on acceptable use and all other applicable SHR policy and federal and provincial legislation.

4.1.3 Manage and maintain their email mailbox.

4.1.4 Use the Email system for purposes that are respectful of others.

4.1.5 Report unacceptable email use immediately to their manager.

4.1.6 Are solely responsible for any material that they access and disseminate through the SHR Email System.

4.2 Managers/Supervisors

4.2.1 Complete SHR User Account application forms to request and terminate e- mail access.

4.2.2 Ensure staff read this policy prior to providing account information.

4.2.3 Use their discretion to restrict email usage, and deny or remove email access for SHR Users for whom they are responsible.

4.2.4 Act on non-compliance or breach of this policy and report such incidents to ITS Security.

4.3 Information Technology Services

4.3.1 Manage and control access to the email system through SHR User Accounts.

4.3.2 Communicate information on potential or known computer viruses.

4.3.3 Send users a warning message when their mailbox has exceeded the allowable mailbox limit.

4.3.4 Monitor all activity and traffic on the SHR network.

4.3.5 Investigate inappropriate or illegal activity on the SHR network and report the findings to an ITS Manager.

4.4 Communications

4.4.1 Are accountable for SHR communication standards, including quality, accuracy and appropriateness of mass or targeted distribution; including criteria for distribution of email messages to "All SHR Users" (3.3 above).

4.4.2 Manage the SHR Email Signature Guidelines and Mass Email Distribution Guidelines.

4.5 Vice Presidents

4.5.1 Are accountable for all email messages distributed to 'All SHR Users' from their respective service line/portfolio. Groups that do not fall under a Vice President's supervision, such as foundations and personnel associations, must meet the criteria for 'All SHR Users' messages.

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

A violation of this policy may result in the suspension or permanent disabling of an SHR User's email account and/or disciplinary action up to and including termination of employment and/or privileges with SHR. Any person who knowingly contravenes HIPA may be subject to a fine of not more than $50,000 and/or not more than one year of imprisonment.[1]

7. REFERENCES

SHR Policies:

- Emailing Personal Health Information
- Password Policy
- SHR User Account

SHR Confidentiality Agreement
Mass Email Distribution Guidelines
Email Signature Guidelines
Additional email information is available on the ITS InfoNet Site under the following sections: "Self Help" and "Frequently Asked Questions"

[1] HIPA Section 64

PROCEDURE Number: 7311-25-005 Title: EMAIL ACCEPTABLE USE	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: Date Approved: November 18, 2011 Date Revised: March 4, 2015 Date Effective: March 10, 2015 Date Reaffirmed: Scope: SHR and Affiliates

1. PURPOSE

The purpose of this procedure is to establish the processes for email access, termination/transfer, computer virus alerts, mailbox maintenance and management, and mass email distribution.

2. PROCEDURE

2.1 Access

2.1.1 The Manager

- Completes a SHR User Account application that includes a request for e-mail access for an employee, physician, other health care professional, student, contractor, vendor, or other person for whom they are responsible and submits to ITS Security.
- At their discretion, can request to have email access removed from a SHR User Account for SHR Users for whom they are responsible by contacting ITS Security.
- May restrict email usage of SHR Users in their department.

2.1.2 SHR User

- New applicants read and sign a copy of the SHR Confidentiality Agreement prior to receiving email access. This document is downloadable from the "Forms" page of the ITS InfoNet site. Always download the most recent copy of this document rather than keeping a copy on file. Note: New SHR employees hired on or after April 27, 2009 will have already signed this form as part of their new employee orientation).

2.1.3 ITS Security

- Process SHR User Account applications received and provide access as requested.
- Disable mailboxes not accessed for 6 months, if no notification has been received (i.e. termination/transfer, LOA). After another **12** months, these mailboxes are backed up and removed.

2.2 Termination/Transfer

2.2.1 The Manager

- Notifies ITS Security on termination/transfer of an employee/SHR User to disable the SHR User Account and email access.
- May request access to the mailbox, as required for business purposes, for up to 3 months.

2.3 Mailbox Maintenance and Management

2.3.1 **SHR Users shall:**

- Check email in a consistent and timely manner.
- Be responsible for mailbox folder maintenance, which includes:
  - Organization and deletion of email from all folders (including their 'Sent' and 'Deleted' mail folders).
  - Deleting email as soon as it is no longer needed
- Know how to unsubscribe from a mailing list that has been subscribed to.
- Whenever practical, store potential email attachments on a network drive, SharePoint site, or other secure location, and hyperlink to the file within the email, rather than attaching the file. (Refer to ITS InfoNet site, "Self Help" section for email for how to insert hyperlinks in an email.)
- ***Never*** use their mailbox to permanently store information. Save emails with required file attachments or personal health information received as follows:
  - File attachments should be saved to a network drive in order to stay within their allowable mailbox limit.
  - Personal health information should become part of the permanent health record. Only ITS shall circulate official statements about computer viruses to SHR Users.

2.4 Computer Viruses

If an SHR User receives a message or chain letter warning about viruses, they should not distribute these warnings. Contact the ITS Service Desk immediately, and they will investigate the potential virus and take appropriate action.

2.5 Distribution of Email Messages to All SHR Users

2.5.1 **SHR User**

- Ensure requests for mass email distribution meet the criteria outlined in policy section 3.3 and the Mass Email Distribution Guidelines.

2.5.2 **Those Authorized to Distribute Mass Email**

- Approve email for distribution based on criteria in the guidelines above.

3. PROCEDURE MANAGEMENT

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

4. NON-COMPLIANCE/BREACH

A violation of this policy may result in the suspension or permanent disabling of an SHR User's email account and/or disciplinary action up to and including termination of employment and/or privileges with SHR. Any person who knowingly contravenes HIPA may be subject to a fine of not more than $50,000 and/or not more than one year of imprisonment.[2]

[2] HIPA Section 64(1)

5. REFERENCES

SHR Policies:

- Emailing Personal Health Information
- Password Policy
- SHR User Account

SHR Confidentiality Agreement
Mass Email Distribution Guidelines
Email Signature Guidelines
Additional email information is available on the ITS InfoNet Site under the following sections: "Self Help" and "Frequently Asked Questions"