CATEGORY:	**INFORMATION TECHNOLOGY**
SUB-CATEGORY:	**APPROPRIATE TECHNOLOGY USE**
GROUP:	
DISTRIBUTION:	**ALL STAFF**
TITLE:	**EMAIL ACCEPTABLE USE**

PURPOSE

The objectives of this policy are to outline appropriate and inappropriate use of Western Health's email system in order to minimize disruptions to services and activities and to comply with applicable policies and laws.

POLICY

Scope

This policy applies to all email users at Western Health (both temporary and permanent), and all Western Health email records.

Account Activation/Termination

Email access at Western Health is controlled through individual accounts and passwords. Each user of Western Health's email system must read and sign the Network Access Form prior to receiving an email access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

All employees of Western Health will receive an email account. Email accounts will be granted to third-party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Credentialed Physicians who are active or associate staff members.
- Contractors
- Students
- Volunteers.

Applications for email accounts must be submitted to Information Technology Help Desk (helpdesk@westernhealth.nl.ca). All terms, conditions, and restrictions governing email use must be in a signed agreement.

Email access will be terminated when the employee or third party terminates their association with Western Health, unless other arrangements are made. Western Health is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased.

Appropriate Use and Management of Email

Individuals at Western Health are encouraged to use email to further the goals and objectives of Western Health. The use of email is appropriate for:

- Communicating with fellow employees or business partners of Western Health, within the context of an individual's assigned responsibilities.
- Communicating with clients or, where applicable, clients' substitute decision – makers.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

Western Health often delivers official communications via email. As a result, employees of Western Health with email accounts must check their email in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling the duties and responsibilities associated with their position.

Western Health employees are permitted to communicate personal health information by email, but only in strict compliance with Policy 10-01-75 Communicating Personal Information by Email.

Email users are responsible for mailbox management, including organization and cleaning. All email users are allotted a specific amount of storage space for their email and it is their responsibility to keep their email storage within that limit.

Email users are encouraged to use the scan-to-email functionality on Western Health's multi-function printers where available as an alternative to faxing or mailing hardcopy documents. Users are to follow the scan-to-email guidelines when using this function.

Email users are expected to remember that email sent from the organization's email accounts reflects on Western Health. All contents of Western Health's email system are

official records of the organization and, as such, are subject to disclosure in the event of an investigation or request whereby the organization is legally authorized or compelled to release records respondent to the investigation or request. An example of this would be a request under *The Access to Information and Protection of Privacy Act*, Policy # 9 – 02 – 50.

Archival copies of all email messages sent from or received in Western Health's email system are retained for at least seven years.

Email users must not intentionally give another user access to their email by revealing their account password. Email transmissions linked to a user's credentials are assumed to be initiated by that user. Should certain content of a particular user's email need to be shared with another person(s) for valid business reasons, the user shall contact the IT Help Desk for assistance. Where appropriate, users are able to assign administrative support staff the ability to manage their mailboxes by providing proxy access.

Western Health staff must not intentionally access the content of another person's email messages without the proper approvals. If such content is accidentally accessed, it must be treated as private and confidential. Any inappropriate inspection of the content of email files constitutes a breach of privacy and will be handled in accordance with the appropriate Human Resource policies.

Generally, email users must comply with normal standards of professional and personal courtesy and conduct when communicating by email.

Inappropriate Use

Western Health's email systems and services must not be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared drive). Email use at Western Health must comply with all applicable laws, all Western Health policies, and all Western Health contracts.

The use of Western Health email system for any of the following activities is strictly prohibited:

- To engage in illegal activities.
- To harass, insult, or malign any person or group
- To receive or distribute materials that might be seen as obscene or degrading
- To misrepresent the truth by knowingly spreading misinformation or posing as someone else.
- To pursue any private commercial purpose.
- To promote non-work-related causes such as political parties or religious organizations.
- To solicit for donations or any other fundraising activities.

- To send chain letters.
- To send non-work-related messages to large audiences.
- To engage in any activity that is in clear conflict with the interests of Western Health or that is in violation with any of the organization's policies.
- Excessive personal use of Western Health email resources. Western Health allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources.

Monitoring and Confidentiality

Western Health reserves the right to monitor the use of the organization's email system for the following purposes:

1. To investigate network performance issues. In this case, the nature and volume of all network traffic may be monitored to identify the cause of network slowdowns or failures. Any instances of inappropriate use discovered in this process will be noted and dealt with accordingly.
2. To confirm or dispel suspicions of excessive personal use or inappropriate use on the part of an individual or group. Monitoring, in this instance, will only be carried out with approval from Senior Management.
3. In the event of an inquiry, investigation, or access to information request where the required legal authority exists.

Email users are asked to take care in directing their messages. Users must only "reply to all" when appropriate and avoid sending repeats of the same message as "reminders." Email users must also ensure the recipient name(s) is correct, and the email must have a subject line.

Only email sent within the WH email system is considered secure. Any external email correspondence containing sensitive information or identifiers must be sent using the secure email functionality. No identifiers are permitted to be part of the subject line. The instructions on how to use secure email are located on the IM Intranet page.

Any email sent to or received from addresses that are not @westernhealth.nl.ca are external to the WH email system. This includes email sent to or received from external persons or entities via an internet email address. Such email is unsecured and cannot be considered confidential unless the secure method is utilized. Therefore, users should be cautious about the type and content of messages they send outside the WH email system.

Third-party email providers (e.g. Hotmail, G-Mail, and other web-based email providers) are external to the organization. WH employees who require access to email must use WH email systems and not their own external accounts.

Users are not permitted to automatically forward their WH email to their personal external account. Personal external accounts are not to be used for the purpose of conducting WH work/business.

Reporting Misuse

Any allegations of misuse must be promptly reported to the Regional Director, Information Management. If you receive an offensive email, do not forward, delete, or reply to the message. Instead, report it directly to the Regional Director, Information Management.

Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at Western Health. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on Western Health's email systems and services may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of email access;
2. Disciplinary action according to applicable Western Health policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.

GUIDELINES

Guidelines for Secure Send Encrypted Email Messages
Guidelines for Using Scan to Email on Western Health Multifunction Printers

KEYWORDS

Email
e-mail
email system
confidentiality
electronic mail
records

TO BE COMPLETED BY STAFF IN QUALITY DEPARTMENT

Approved By: Chief Executive Officer	Maintained By: Provincial Manager-Application Development, Solutions and Infrastructure
Effective Date: 07/June/2012	☑ Reviewed: 20/October/2020 ☑ Revised: 14/December/2017
Review Date: 20/October/2023	❒ Replaces: *(Indicates name and number of policy being replaced)* OR ☑ New