Acceptable Use of Information Systems		
For Policy Office Use Only		
☑ **Administrative** ☐ **Clinical**		**Policy Number:** 10357
Approved By: Executive Team **Approval Date: February 15, 2022** **Effective Date: February 15, 2022**	**Original Date: September 2009** **Revised Date(s): February 15, 2022** **Next Review Date: February 15, 2026**	**Version: 3**
All Rights Reserved. This is a CONTROLLED document for internal use only. Any documents appearing in paper form are not controlled and should ALWAYS be checked against the electronic version prior to use.		
Policy Sponsor: Vice-President Quality, Strategy and Family Partnership		
Policy Author: Brian Vezina		**Dept**: IS
Scope/Impact: *All Information Systems and services owned, leased, or in the custody of the CHEO; All Information Systems account Users/holders at the CHEO; All CHEO Information Systems records. Information Services does not support in-house developed applications such as Microsoft Access Databases. There are two service levels for off the shelf software, supported and limited support. Other software packages are considered to be prohibited.*		
Keywords: Expectations; Personal Files; Personal Folders; e-mail; Internet; Remote Access; Removable Media; Portable Devices		

1. PURPOSE:

1.1 To outline the appropriate use of information systems including services such as use of e-mail, internet and remote access services.

1.2 To provide guidance including general expectations of users and their responsibilities in ensuring the computer services are used in an effective, ethical, secure, and lawful manner.

1.3 To ensure the safe and respectful use of information systems and services.

2. POLICY:

2.1 General Use

- Use of information systems is an essential means for doing business at CHEO. These services must be used with respect and in accordance with the applicable rules and legislation to further the goals of CHEO.
- There are two (2) prerequisites to becoming a User of CHEO information systems and services:
- The individual must sign CHEO's Confidentiality Agreement (Form No #6021 E/F))
- The individual's director must complete and sign the Information Services Citrix Access Control form (Form No #6043) requesting access to those applications and access type.

Once the prerequisites have been met, the individual is a User. Some departments may have Super Users. Super Users are an internal department resource that are available to assist staff with access and general use of information systems.

For more information on any of the systems or services, please consult the Helpdesk resources available on the CHEO information services CHEOnet page.

2.2 General Expectations of Users

As CHEO often delivers official communications via e-mail or by posting to the Corporate Intranet site (CHEOnet) all users are:

- Expected to check their e-mail and the corporate intranet site in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling business and role-oriented tasks.
- Encouraged to use information systems to further the goals and objectives of the organization. The types of activities that are encouraged, but not limited to, include communicating with fellow CHEO Users, business partners of CHEO, and clients within the context of an individual's assigned responsibilities; acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and participating in educational or professional development activities.
- Expected to perform effective file and e-mail message management, including but not limited to file organizing, cleaning, purging, archiving and maintaining their storage quota.
- To use information systems in accordance with CHEO policies, rules, or administrative orders.
- Permitted a limited personal use of CHEO Information Systems 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.
- To complete annual mandatory cybersecurity training.

2.3 Passwords

- All users must choose passwords used to access Information Systems that are easy to remember but hard to guess by someone else. Users are required to:
- Change their windows login password every 180 days. This password must include the following minimum complexity requirements:
- at least eight (8) characters in length.
- at least one (1) uppercase character
- at least one (1) lowercase character
- at least one (1) number
- Users must never create passwords used to access CHEO Information Technology resources that include:
- All or part of their user name
- Easily obtained personal information about themselves (e.g., names of family members, pets, birthdays, anniversaries, hobbies)
- Three consecutive characters (e.g., AAA).
- Where possible, users should use phrases when creating passwords used to access Information Systems.
- Safeguard their system passwords and are not to disclose their system access credentials to anyone, even Information Services personnel.
- Passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons may discover them.
- If a user believes that their user id and password have been compromised, the user must immediately change their password and report the suspicion to their immediate supervisor.

- In the event the account compromise is detected by Information Services, the account will be disabled immediately.
- In the event a password has been forgotten or expired, the User must present themselves to the IS Helpdesk along with photo identification to have their password reset.

2.4 Personal Files and Folders:

- A personal folder will be established for each User with a storage quota of 1,000 MB. Additional space must be justified by the User and authorized by the User's Director. User are expected to:
- Expected to secure their account while logged in by "locking" their active computer session when leaving computer unattended as well as to log off their account at the end of their shift/work day.
- To only attempt to gain access to any information systems or services for which they have explicit authorization through a signed Information Systems Citrix Access to Control form.
- Users **are not** permitted to remove or install software to CHEO's information systems without the authorization of Information Services (IS).
- Any issues encountered with CHEO information systems or services should be reported promptly to the IS Helpdesk by either webform or telephone. An Incident number will be issued by the Technical Support Analyst to ensure proper tracking and resolution.

2.5 E-mail:

- A mailbox will be established for each User with a storage quota of 280 MB. The User will receive a warning message when they reach this limit. If no action is taken and the mailbox size continues to grow, the User may stop being able to send or receive e-mails. If this happens the senders will receive automatic reply that the recipient's mailbox is full.
- All Health Care Providers must follow their College scope of practice or service regarding the use of electronic mail for communicating Personal Health Information (Privacy and Confidentiality of Personal Health Information). E-mail of personal health information is strictly prohibited unless a Patient Consent for e-mail Communication (Form No. F6240 has been obtained from the patient or substitute decision maker.
- All Users must never use external email accounts (e.g., Hotmail, or Gmail) to send or receive Personal Health Information. Similarly, external personal instant messaging and text applications are also prohibited for communication personal health information.
- CHEO prohibits personal use of its e-mail system for unsolicited mass mailings, non-Hospital commercial activity, political campaigning, dissemination of chain letters, or use by non-users.
- CHEO is not responsible for any third-party claim, demand, or damage arising out of the use of CHEO information systems or services. CHEO assumes no liability for direct and/or indirect damages arising from the User's use of the Organization's information systems and services.
- All electronic mail messages sent from their Hospital account(s) reflects on CHEO's corporate image and are therefore required to comply with normal standards of professional and personal courtesy and conduct. Users are:
- Not **to** open e-mail attachments from unknown or unsigned sources as attachments are the primary source of computer viruses and should be treated with utmost caution.
- Not **to** take a picture of data displayed on any computer screen.

- To be extremely cautious when:

  2.5.1 Communicating confidential or sensitive information via e-mail. Keep in mind that all electronic mail messages sent outside of CHEO become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "reply all" command during information systems correspondence to ensure the resulting message is not delivered to unintended recipients.

  2.5.2 Sending message to external recipients to ensure the information is transmitted to the intended person. It is good practice to ask the intended recipient to respond to an acknowledgement message before sending business correspondence to ensure confirm the accuracy of their address.

  2.5.3 To ensure the information being transmitted is appropriate for all recipients when responding to a message and including additional recipients. Often messages have a trail of iterations and that may not wish to be shared.

- If inappropriate material is received from an external source known to staff, it is the User's responsibility to contact the source and inform them that such material must not be sent to anyone at CHEO. The material must be deleted from the user's mailbox immediately.

- Diligence needs to be exercised when dealing with junk email or spam as some emails contain viruses or are fraudulent. Spam cannot be completely blocked thus placing the onus on users to use their best judgement when responding to these types of emails.

- To access their e-mail from a remote location via CHEO webmail or other remote access tools if authorized.

- To safeguard any corporate information they copy or synchronize to portable personal devices (i.e. memory sticks, external hard disks, personal digital assistants (PDAs) or Smartphones). If copying or synchronization is required in the due course of performing job duties, CHEO will provide the User with approved portable devices with proper encryption.

- When required to leave a portable computing device in a vehicle, all users must lock the device in the trunk or place it out of view.

- The following disclaimer appended to all external bound messages as a safeguard against messages reaching unintended recipients.

  " This message, including any attachments, may contain confidential information and is for the sole use of the intended recipient(s). Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please notify the sender immediately and destroy the original message (for further detail please see http://www.cheo.on.ca/en/disclaimer).

  Ce message, y compris les pièces jointes, peut contenir des renseignements confidentiels, et seuls les destinataires visés peuvent le consulter. Il est strictement interdit de l'utiliser sans autorisation, de le divulguer ou de le distribuer. Si ce message ne vous était pas destiné, veuillez en informer l'expéditeur immédiatement et détruire le message original (Veuillez consultez http://www.cheo.on.ca/avis-non-responsabilite pour plus de précisions). "

2.6 Internet Use:

- The homepage on all CHEO information system devices must be set to the Corporate Intranet Homepage (CHEOnet). This helps promote awareness of important CHEO announcements and communication. The Internet is a public forum for business communication and reflects on the Organization's corporate image and its place in the community. All Users are responsible to maintain and enhance CHEO's public image.

- CHEO reserves the right to restrict access to internet sites it considers inappropriate for the workplace.
- CHEO may restrict Internet access for any User if a supervisor believes that this privilege has been detrimental to the User's productivity on the job.
- Each internet user is responsible for the internet activity performed under their account.
- Downloading software, such as shareware, bulletin software or games from the internet to CHEO information systems is not permitted.

2.7 Remote Access:

- All CHEO users are provided with remote access to Outlook Web Access, the Corporate Intranet (CHEOnet), Staffing and Scheduling Portal (ESS) and Employee Information Centre (Online Pay Advice) resources via www.cheo.on.ca/help.
- Full remote access via Citrix is a powerful privilege that allows users to have access to all applications and patient data from anywhere on any device. Full remote access must be authorized by the user's Director through the "Information Systems Access Control" form forwarded to CHEO IS Helpdesk indicating remote access is a requirement for user to fulfill their job requirements. Users may be authorized by their Director to access CHEO information systems and services from a remote location by requesting this privilege via the Information Services Citrix Access Control form (Form No.6043).
- Users expected to store sensitive Hospital documents and other printed materials securely in accordance with the Hospitals' "Confidentiality Agreement" (Form No. 6021) while working from a remote location.
- Users of personal devices, must ensure their device is configured to lock the screen with a password if left unattended for more than 20 minutes.
- Users must disable any automatic log-in tools when connecting to the Hospital's information systems from a remote location and if using personal devices.
- Users are expected to use a personal firewall on any computer system used to remotely access the Hospital's information systems. Personal firewall settings are enabled by default on all Hospital devices with this functionality. For more information on enabling personal firewall on their personal devices, Users are encouraged to contact either their equipment manufacturer or Internet Service Provider.

2.8 Portable Devices and Removable Media:

- Users are Strongly discouraged and should avoid saving any sensitive information outside the designated locations.
- To take appropriate steps to protect the information by (1) Password-protected files (The password should be communicated over the phone or in separate email), (2) encrypted media (3) de-identifying the information (4) Transmit over approved secure communication (VPN) (5) ensure a copy of the information resides in the designated location for proper backup, and (6) if e-mail or other data is synchronized to a personal device, that the device itself is password protected and encrypted.
- To affix an "If Found, please call" label to any portable device or removable media.

- Lost or stolen portable devices and removable media must be reported as an incident immediately to user's immediate supervisor, Security and the IS Helpdesk.
- All portable and removable media is to be encrypted.

2.9 Virus Protection and Security Updates:

- Virus infections represent a serious threat to the operation of CHEO and its data. All users are expected to take reasonable precautions to protect against the spread of computer viruses. This includes scanning of disks, removable drives and software for viruses and immediately informing their supervisor if a virus has been discovered.
- All CHEO computers are equipped with antivirus software and firewall.
- Virus definitions and system security updates are updated regularly. Some updates will prompt for user action such as system restart or acknowledgement. These actions are to be treated as a priority and therefore, should not be deferred for extended periods.

2.10 Compliance monitoring:

- All user activity investigation must be authorized by Human Resources.
- If CHEO discovers or has sufficient reason to suspect activities that do not comply with applicable laws or this policy, information systems records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify the User if his or her information system records are to be reviewed. Notification may not be possible, however, if the User cannot be contacted or if notification will defeat the purpose of an ongoing investigation.
- All users must provide their full cooperation to Information Services Department with any information security incident investigation.
- The information systems and services used at CHEO are owned, leased, or in the custody of the organization and are therefore its property. This gives CHEO the right to monitor any and all information traffic passing through its systems. This monitoring may include, but is not limited to, inadvertent reading by Information Services staff during the normal course of managing the information system, review by the legal team during the information system discovery phase of litigation, observation by management in cases of suspected abuse or to monitor user efficiency.
- Violations of this policy will be treated like other allegations of wrongdoing at CHEO. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on the CHEO's information systems and services may include, but are not limited to, one or more of the following:
- Temporary or permanent revocation of information systems access
- Disciplinary action according to applicable CHEO policies
- Termination of employment; and/or legal action according to applicable laws and contractual agreements.

3. RESPONSIBILITIES:

3.1 Users are responsible for:

- Signing the “Confidentiality Agreement” form
- Only using their own password to access systems
- Checking e-mail and corporate intranet regularly

- Performing effective file and e-mail management
- Using e-mail system and internet appropriately
- Reporting any issues to the Information Services Helpdesk
- Changing their password every 180 days
- Safeguarding their password
- Locking workstation while unattended
- Logging off their account at the end of work day or shift
- Taking all appropriate precautions outlined in this policy
- Reporting any breaches or infractions to their immediate supervisor
- Completing annual cybersecurity training.

3.2 Department Directors and Managers are responsible for:

- Authorizing access and signing the Information Services Citrix Access Control form
- Authorizing increase in space quotas
- Follow up if disciplinary action is required

3.3 Technical Support Analyst is responsible for:

- Following up with the User when issues are reported

4. PROCEDURE:

4.1 Reporting Issues with Information Systems:

4.1.1 The User must contact the IS Helpdesk via e-mail, telephone or walk-in.

4.1.2 Upon logging your incident, a Technical Support Analyst will issue you an incident number.

4.1.3 The incident will be placed in a queue that will be addressed depending on the severity and urgency of the issue. Helpdesk assigns patient care related calls higher priority.

4.1.4 The User will also receive an automated e-mail confirmation from the IS Helpdesk with the reference number assigned to the incident.

4.1.5 The Technical Support Analyst will contact the User if additional information is required.

- Make two attempts to contact you (phone or e-mail) using information you provided upon reporting your incident. If the analyst does not receive a communication back from you within five business days from the last contact, the ticket will be closed.
- When the Technical Support Analyst resolves the incident, they will follow up with you via phone or email to confirm the incident has been resolved.

4.1.6 All privacy breaches, allegations of misuse, offensive e-mail (do not forward, delete, or reply to the message) should be promptly reported to your immediate supervisor.

5. CROSS-REFERENCES:

CHEO Policy, Access Control to Information Systems
CHEO Policy, Ethical Code and Conduct and Reporting
CHEO Policy, Privacy and Confidentiality of Patient Protected Health Information
CHEO Policy, Retention and Destruction Of Patient Health Records
Confidentiality Agreement (Form No. 6021 E/F)

Information Services Citrix Access Control Form (Form No. 6043)

6. REFERENCES:

Acceptable Use Policy. eHealth Ontario. Retrieved form the wed: July 2012 www.ehealthontario.on.ca
Information Technology Adviser Publications 2012

7. APPENDICES:

Appendix A: E-mail Etiquette Guidelines

Appendix B: Helpdesk Information Guide

8. DEFINITIONS:

Acceptable Use: Users are permitted to use CHEO's information systems and services.

Designated locations: are network file shares (example: J:\ Drive).

Electronic mail (e-mail): is any method of creating, transmitting, or storing primarily text-based human communications with digital communications systems.

Firewall: a dedicated appliance or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

Individual: Any person who does not meet the criteria of a "User".

Information Systems: any computerized data processing or storage system. Any telecommunications system whose function is to transmit and/or display data.

Internet: a global system of interconnected computer networks that interchange data by packet switching using the standardized Internet Protocol Suite (TCP/IP). It is a "network of networks" that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies.

IT Equipment: any computing hardware used to access, process and store or transmit Hospital information (example: PC or server). Portable IT equipment includes laptop, tablet PC, handhelds and smartphones.

Limited Support: User deals directly with Vendor and understands the terms and conditions outlined in Disclaimer. CHEO IS involvement is limited to assistance with installation, provide infrastructure to run application (Network Share Backup), software asset management (license management).

Personal Devices: any computing hardware used to access, process and store or transmit Hospital information (example: PC, smartphone or tablet) that is property of the user and has not been configured by CHEO Information Services.

Personal Firewall: an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. This differs from a conventional firewall in terms of scale and is typically designed for use by end-users. As a result, a personal firewall will usually protect only the computer on which it is installed.

Prohibited Software: Any package not appearing on Supported or Unsupported list is deemed to be Prohibited. These packages are not conforming to CHEO Standards, known to be toxic to environment, or malicious code.

Protected Health Information (PHI): is identifying information about an individual that, (a) relates to the physical or mental health of the individual, including health history of the individual's family, (b) relates to the providing of health care to the individual, including the identification of the care provider (c) relates to payments or eligibility for health care in respect of the individual, (d) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, (e) is the individual's health number, or (f) identifies an individual's substitute decision-maker.

Supported: CHEO Support Aligned (Full Lifecycle Management)

Remote Access: Is the ability to access a CHEO computer, network drive, or application from a remote location. Remote access is applicable to many forms of connectivity methodologies including but not limited to dial-up, VPN, and Citrix.

User: An individual who has authorized access to the Children's Hospital of Eastern Ontario's information systems and has signed the Acceptable Use of Information Systems Agreement.

Version History:

Date	List of minor revisions	List of major revisions
24/07/2019	Revisions for 2019-20 Review.	
15/02/2022		Address EMRAM requirements to achieve HiMSS level 7 Corporate Priority