PPG-00061

ICT Acceptable Use

Area	Information and Communications Technology
Section	Computer Users
Subsection	N/A
Document Type	Policy
Scope	APPLIES TO ALL PMH EMPLOYEES

Approved By	**Original Effective Date**	**Revised Effective Date**	**Reviewed Date**
Penny Gilson, CEO EMT meeting 2017-Nov-14	2014-Jun-02	2018-Mar-14	2018-Mar-14

This policy follows a standard provincial template and any major changes should be reviewed by the Provincial ICT Operations Working Group

DEFINITIONS

Confidential Information: includes, but is not limited to: Personal health information as defined in *The Personal Health Information Act (PHIA);* Personal information as defined in *The Freedom of Information and Protection of Privacy Act (FIPPA*), and; Administrative records collected and created as part of the course of business of Prairie Mountain Health and relate to legal, financial and operational matters of a confidential nature.
Encryption: a method of converting data to a secure and unreadable format. Data can only be read by an individual who has the "key" to unscramble the code (e.g. a password).

ICT Resource Disruption: Disruptions include, but are not limited to:

- Propagation of computer viruses, worms, spyware, malware, Trojan horses, email bombs, etc.
- Disconnection of, or damage to equipment or services
- Disruption of network traffic causing loss of service, including excessive bandwidth or excessive use of computer resources
- Rogue modems and/or wireless access points
- Port scanning or security scanning
- Network monitoring that intercepts data not intended for the use outside normal job responsibilities
- Change to the system or data configuration that could affect system integrity

ICT: refers to the Information and Communications Technology department

Information and Communications Technology (ICT) Resources: all assets relating to information and communications technology including, but not limited to, all information in electronic form (e.g. personal health information) and the hardware, software or network components on which information is entered processed, stored or transmitted

Information and Communications Technology (ICT) Services: includes all Prairie Mountain Health internet, email, network and telecommunication services

Objectionable Material: includes but is not limited to:

- obscene or pornographic material
- hate propaganda or discriminatory material
- defamation and libel
- sexual harassment
- offending pictures and jokes
- messages where the meaning is likely to be highly offensive to the recipients of the message

Persons associated with Prairie Mountain Health: includes Prairie Mountain Health medical staff, contracted persons, volunteers, students, researchers, educators, and Board members.

Portable Electronic Devices (PEDs): Portable information systems or devices with the capabilities of recording, storing, processing and/or transmitting electronic data. These include, but are not limited to, laptops, smart phones, tablets, memory sticks, cellular phones, pagers and other similar devices.

Portable Storage Media: hardware devices used to store information. This includes, but is not limited to USB storage devices (e.g. memory stick, flash drive), CD/DVD, etc.

Remote Location: a physical location outside your normal office or work location

Security Incident: an action by an authorized or unauthorized user or an event that may negatively impact or cause interruption, unauthorized access, modification, destruction or denial of service

Privacy Incident: incidents where the confidentiality, security, accuracy and/or integrity of confidential information has been compromised.

Social Media: Internet-based applications that allow the creation and exchange of user-generated content. This includes, but is not limited to websites such as Facebook, Twitter, YouTube, LinkedIn and MySpace.

Streaming: Connecting via the network to listen to radio stations or viewing videos or webcasts

Transitory/working emails/documents: Messages/documents of short-term use and significance that are not required as part of a required record maintenance system once read or superseded. (I.e. meeting requests, messages that are not required as evidence of the decision making process)

User: Individual who is authorized to access Prairie Mountain Health's ICT Systems.

User ID: a unique personal network/system identification (e.g. username).

Virus or Malware: any program designed to copy itself into other programs often resulting in the alteration/loss of data and/or the disabling of computers and networks

POLICY STATEMENT

1. ICT resources are intended for business use only.

2. Prairie Mountain Health reserves the right to monitor, review, access and/or block user activity without user notification.

3. Users are responsible for all activity while logged in under their assigned network user ID and password.

4. Any material created, stored, sent or received using ICT resources are considered the property of Prairie Mountain Health.

5. All users have a legal and ethical duty to protect the confidentiality, integrity and availability of all electronic information.

6. Access to information systems and data is restricted to authorized users and is limited to that which the user requires to do their job.

7. Prairie Mountain Health will report to and cooperate with law enforcement where activities or reports of activities are considered illegal.

8. The ICT acceptable use policy extends to any off site or remote locations (e.g. working from home).

PROCEDURE/RESPONSIBILITIES

1. Protecting ICT Resources

1.1. Users apply appropriate precautions to prevent loss, damage, theft and/or unauthorized access to ICT resources
1.2. Computer sessions are logged-off or locked when the user is away from the workstation, to prevent unauthorized access
1.3. Individual passwords are not shared.
1.4. Passwords for generic/shared accounts are kept secure and only available as required to perform work duties
1.5. Only the user assigned user ID and password are used for system access.
1.6. Compromised passwords are changed promptly and reported by phone to the eHealth service desk as a Critical Ticket
1.7. Approval is obtained from the ICT for use and/or installation of new software and hardware
1.8. Suspicious files/programs or messages encountered while using ICT resources are reported to ICT
1.9. Lost or stolen ICT resources are immediately reported to the ICT
1.10. ICT is contacted where ICT equipment is moved/relocated to another office/program/facility
1.11. Intentional and/or malicious disruption to ICT services is prohibited

2. Confidentiality

2.1. Users are responsible for proper storage (e.g. secure network folder) and security of all confidential information
2.2. Confidential information is not stored on a local computer (C :) drive or on any portable storage media unless it is encrypted and/or password protected. (Note: Information stored on a local computer (C :) drive or portable storage media is not protected by automatic back-up processes.)
2.3. Access to information stored in a network storage location is restricted to users who require the information to do their job

3. Email

3.1. Email is created and used in a professional manner

Note: Email created in the course of carrying out Prairie Mountain Health duties are considered business records and access may be requested by any person under *The Freedom of Information and Protection of Privacy Act (FIPPA).*

3.2. Confidential information is not sent to an email address other than @pmh-mb.ca unless it has been secured (e.g. Encrypted). If assistance is required contact ICT. Exceptions to this rule are:
- When email is the only timely way to send information that is required urgently and informed consent has been documented and obtained from the appropriate individual.
- When the purpose is for scheduling appointments where the individual has requested or agreed to receive this information by email and has provided their email address
- When the organization receiving the email has an established secure connection with Prairie Mountain Health. ICT maintains and posts a current list of those organizations.

3.3. Users open only email and attachments from a trusted or verified source. Email attachments from unknown sources should be promptly deleted, unopened.
3.4. In the event of accidentally opening a suspicious attachment, report this by phone to the eHealth Service Desk as a Critical Ticket.
3.5. Confidential work related information is not forwarded to personal email addresses or any other non-work related accounts.
3.6. Email messages are not forged or altered to impersonate another individual or entity
3.7. Email folders (e.g. Inbox, Sent) are managed by routinely deleting unnecessary items and/or the use of archive folders in accordance with ICT guidelines.
3.8. Email addresses and contact names are verified prior to sending/forwarding email messages.
3.9. Email that contains defamatory, offensive, racist or obscene remarks is prohibited and users, who receive an email of this nature, notify their supervisor/manager.
3.10. Email signatures include, at minimum, name, job title and /program name, in accordance to ICT guidelines.
3.11. Use of spellchecker prior to sending email is strongly encouraged
3.12. Sending/forwarding of chain letters, junk mail, mass personal mailings, alleged virus alerts or other SPAM is not permitted
3.13. Forwarding jokes is discouraged

4. Internet

4.1. Confidential information is not transmitted over the Internet unless it has been secured (e.g. encrypted).
4.2. Accessing, viewing, downloading or distributing objectionable material is prohibited.
4.3. Unauthorized Internet use includes, but is not limited to:
- audio and video streaming not required for work,
- gaming,
- peer to peer file sharing,
- music downloading not required for work,
- gambling

4.4 Social Media

4.4.1 Access to external social media sites may be blocked on the Prairie Mountain Health network. Users may be granted access to blocked sites for work-related business or for education purposes where authorized by their Manager\Director.

4.4.2 All employees and persons associated with Prairie Mountain Health, who participate on social media sites, are responsible for the information posted and represent Prairie Mountain Health in a respectful, professional manner.

4.4.3 Only those employees and persons associated with the Prairie Mountain Health who are duly authorized to make statements to the public/media on behalf of Prairie Mountain Health may communicate via social media

4.4.4 Posting/communicating any of the following material on a social media site is strictly prohibited:
4.4.5 Information about clients (e.g. images, personal health information) or co-workers
4.4.6 Defamatory, damaging or embarrassing comments about Prairie Mountain Health, its services, employees or any persons associated with Prairie Mountain Health.
4.4.7 Confidential or proprietary information that may compromise Prairie Mountain Health business practices or security
4.4.8 Content that could bring Prairie Mountain Health into disrepute or that has the potential to damage the Prairie Mountain Health reputation.

5. Personal Use

5.1. Personal use of ICT resources/services (e.g. email or Internet) is limited to break time and does not interfere with work
5.2. Conducting or pursuing personal business interests or those of another organization while using ICT resources is prohibited
5.3. Personal files stored on the network are routinely deleted

6. Portable Electronic Devices (PEDs)

6.1. Screen savers are set to password protect the PED after a maximum of 20 minutes
6.2. Users take steps to prevent unauthorized viewing of the computer screen/display
6.3. PEDs are not left unattended unless physically secured
6.4. A security cable is used for PEDs kept in unsupervised locations. Where a PED has no place to attach a cable, the device is placed in a secure storage location.
6.5. PEDs are stored in a secure location when taken home
6.6. PEDs are not left in a vehicle
6.7. When traveling by plane, taxi or train, verify that you have the PED and the case, including all contents, prior to exiting
6.8. PEDs are kept in sight when going through airport security checkpoints
6.9. Users only connect to an identified wireless network to which the source is known. For example, when in a hotel use the hotels wireless connection provided to you. Do not connect to “unknown” or “suspicious” networks.
6.10. PEDs are locked in the room safe, where provided by the hotel

7. Portable Storage Media

7.1. Portable storage media is encrypted and/or password protected
7.2. Portable storage media is ordered through ICT to ensure it meets ICT standards for secure devices.
7.3. Use of other types of personal portable storage media is discouraged and may be monitored and/or blocked
7.4. Vendors and presenters using portable storage media are advised that the files on the device be subject to Prairie Mountain Health anti-virus scanning.

8. Privacy and Security Incidents

8.1. Immediate steps are taken to contain an incident by securing and/or recovering any compromised ICT resources.
8.2. All incidents or potential compromise to the confidentiality, security, integrity or availability of ICT resources is immediately reported to the Regional Manager – ICT and/or Regional Manager – Access & Privacy.
8.3. Misuse of ICT resources/services by any user is reported to their immediate

RELATED MATERIAL

PPG-00062, Password Policies
PPG-00179, Confidentiality
PPG-00189, Conflict of Interest
PPG-01365, ICT Security
Email Signature Block Guidelines
PMH2041, Social Media Tips & Tricks

DOCUMENT HISTORY

Version	Changes
2014-Jun-02	New.
2018-Mar-14	Revised. Updated policy to align with Provincial Template.