cpsa

COLLEGE OF PHYSICIANS
& SURGEONS OF ALBERTA

Privacy Directive
Acceptable uses of networks & electronic devices

1. PURPOSE

This Privacy Directive outlines the requirements and expectations of CPSA team members when accessing CPSA electronic systems, whether working at the office or through remote access. If you require an exception to this directive, you must obtain approval from your Leadership Team member in advance and in writing.

2. DEFINITIONS

Definitions of terms used in this directive are in section 2 of the *Privacy and Confidential Information Policy*; additional definitions include:

Electronic systems: electronic environments, networks, applications, and electronic devices

Malware:

- Adware: any software which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it.
- Keylogging: the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
- Spyware: malicious software that is installed on computers and that collects information about users without their knowledge.
- Trojan horse: malicious software that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- Virus: a computer program that can copy itself and infect a computer, corrupting or destroying files on that computer.
- Worm: a self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention.

3. GENERAL REQUIREMENTS

You are responsible for exercising good judgment regarding appropriate use of resources in accordance with CPSA policies, directives, standards and guidelines. CPSA prohibits any unlawful use of CPSA resources.

For security, compliance and maintenance purposes, authorized IM team members may monitor and audit our electronic systems. If IM finds a device or user interfering with our electronic systems, the device (or the user's access) may be disconnected.

4. SYSTEM ACCOUNTS & ELECTRONIC DEVICES

a. You are responsible for the security of data, accounts and systems under your control.

b. You must keep all passwords confidential and secure.

c. It's unacceptable to provide access to another individual, either deliberately or through failure to secure your account or device access.

d. CPSA prohibits any team member and/or vendor from storing any confidential information on private devices and/or within non-CPSA controlled or authorized environments. This includes devices maintained by third parties with whom CPSA does not have a contractual relationship.

e. You must secure your devices including computers, smart phones, laptops, and workstations with a password-protected screensaver. It's your responsibility to lock your screen or log off when a device is unattended.

f. Unless authorized by your Leadership Team member, you cannot use mobile devices such as flash drives to store or transport confidential information, including personal and/or health information.

g. If CPSA authorizes a mobile device for storing, accessing and/or transporting sensitive data, you must encrypt the data.

h. Upon employment termination with CPSA, you must return all access control items and information assets belonging to the CPSA. This also applies to vendors when their contractual or business relationship ends with CPSA.

5. COMPUTING ASSETS

a. You are responsible for ensuring the protection of any assigned assets and must report any theft or loss of those assets immediately.

b. CPSA strictly prohibits any interference with its device management or security system software, including but not limited to antivirus software.

c. Installation of any software on CPSA equipment must be approved in accordance with CPSA's *Software Standards* policy.

6. USE OF PRIVATE DEVICES

a. When permitted under the IT *Remote Access* policy, you may use a private device to access CPSA systems and information (e.g., email accounts, SharePoint, Remote Desktop).

b. While you maintain your rights to your private device, CPSA retains all rights to CPSA systems and information accessed.

c. Any private device you use for CPSA business is subject to all CPSA policies, and must comply with information management requirements (e.g., such devices must be password protected and maintain virus protection).

d. You must take great care when repurposing or disposing of your private devices used for CPSA business. This ensures a third party does not access information inadvertently.

   i. Ensure you securely overwrite or strip repurposed devices using industry standards.

   ii. Dispose of all devices using secure means (e.g., using certified hardware disposal organizations).

   iii. The Chief Information Officer is available to all current and former employees who require guidance on safe device disposal.

7. NETWORK USE

a. You are responsible for the security and appropriate use of network resources under your control.

b. CPSA prohibits the following uses of networks and/or resources:

   i. Breaching security, including but not limited to accessing data, servers, or accounts without authorization and circumventing user authentication on any device.

   ii. Intentionally and/or maliciously disrupting services.

   iii. All violations of copyright law, including but not limited to illegally duplicating or transmitting copyrighted pictures, music, video and software. Exporting or importing software, technical information, encryption software or technology in violation of international or regional export control laws.

   iv. Use of the Internet or network that violates organizational policies or local laws.

   v. The intentional introduction of malicious code or malware.

8. ELECTRONIC COMMUNICATIONS

CPSA strictly prohibits the following:

a. The use of email accounts not provided or approved by CPSA to conduct organizational business.

b. Inappropriate use of communication vehicles and equipment, including but not limited to supporting illegal activities and procuring or transmitting material that violates organizational policies against harassment or the safeguarding of information.

c. Sending spam via email, text messages, pages, instant messages, voice mail or other forms of electronic communication.

d. Forging, misrepresenting, obscuring, suppressing or replacing a user identity on any electronic communication to mislead the recipient about the sender.

e. Posting the same or similar non-business-related messages to large numbers of groups.

f. Use of a CPSA email or IP address to engage in conduct that is ethically questionable, unlawful or violates CPSA policies and protocols.

9. COMPLIANCE

Team member (except for council/committee members) or vendor failure to comply with this policy is cause for disciplinary action up to and including termination of employment or business relationship and, where applicable, legal or other action. Council/Committee members' failure to comply with this policy is addressed by the council president.

Please direct any questions or concerns about CPSA's handling of confidential information to CPSA's Privacy Team.

10. REFERENCES

This directive falls under the *Privacy and Confidential Information Policy*.

Related Policies

- *Artificial Intelligence*
- *Internet Access & Use*
- *Prevention and Detection of Theft and Fraud*
- *Records and Information Management*
- *Software Standards*
- *Team Member Code of Ethics*

Privacy Directives

- *Access to Personal Information*
- *Privacy and Information Management Training*
- *Protecting Confidential Information*
- *Protecting Information when Contracting for Services*
- *Team Member Arrival/Departure*

Privacy How-to Sheets

- *Auto-Complete Settings in Outlook*
- *Locking & Securing Computers*
- *Privacy Breach Response*
- *Recording Audio or Videoconferences*
- *Secure Printing*
- *Sharing Confidential Information Electronically*

IT How-to sheets

- *Set-up Remote Access*