AR0600 – INTERNET ACCESS

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

To set standards for using the Internet access provided by Interior Health (IH), and the appropriate use of systems accessing the Internet to protect the confidentiality, integrity and availability of IH data and systems.

2.0 DEFINITIONS

TERM	DEFINITION
Confidential Information	*In this policy, confidential information refers to:* *a) Any electronic information that identifies an individual or that can be combined with other information to identify an individual. This definition applies to anyone, living or dead, and includes information such as patient/client address, telephone number and personal health card number (PHN).* *b) Any electronic corporate information which has not been authorized for disclosure.*
Internet	*A network of computer networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. Most often accessed through a web browser such as Microsoft Edge or Google Chrome.*
Offensive material	*Includes pornography, hate literature or any material which contravenes the BC Human Rights Act.*

User	*Includes all staff, physicians, independent contractors, students, volunteers, and any other persons acting on behalf of IH.*

3.0 POLICY

3.1 Use of the Internet

Users must not:

- Access sites that carry offensive material.
- Download files, including software, screen savers, or media (music, video, standalone executable) files.
- Use their personal Internet based email systems such as Hotmail, Yahoo, or Gmail for work related business.
- Use Internet based game sites or download games.
- Use social networking sites other than for work related business. All postings must comply with the IH Social Media policy and guidelines.
- Transmit confidential information via the Internet unless the information is encrypted in compliance with the BC Ministries of Health approved standards.
- Attempt to obscure the origin of any message or download material under an assumed Internet address.

3.2 Personal Use

Although the computer system is provided to the user for the purpose of business functions, a limited amount of personal use is permitted, on the following understanding:

a) The computer and everything it contains including data files and email is the property of IH and may be subject to auditing and Freedom of Information access requests.

b) Personal use will not:
   a. Interfere with work productivity.
   b. Disrupt the system and/or harm the reputation of IH.
   c. Violate this or any other IH agreement or policy.
   d. Involve any private business activities.

3.3 Compliance

Failure to comply with acceptable use standards may lead to termination of access, employment and/or contract, withdrawal of privileges in accordance with Medical Staff Bylaws, and /or professional sanctions.

4.0 PROCEDURES

4.1 All Users will:

- Accept the appropriate data access and confidentiality acknowledgement prior to being granted access to the Interior Health information system.

4.2 Manager / Chief of Staff will:

- Agree to this Policy annually.
- Follow-up on compliance audits in consultation with Human Resources and/or Executive Medical Directors and take appropriate action when required.

4.3 Digital Health will:

- Ensure controls are in place to prevent threats from compromising the computer system.
- Conduct regular audits to ensure compliance.

5.0 REFERENCES

1. IH Policy: AR0100 Acceptable Use Policy
2. IH Policy: AR0500 Email
3. IH Policy: AR0400 Privacy and Management of Confidential Information
4. IH Policy: AR1000 Social Media
5. IH Policy: AU0100 Standards of Conduct
6. Social Media Guidelines
7. Medical Bylaws