Information Technology: Acceptable Use of

1. Introduction

Information Technology enables PHC to deliver health care services efficiently and effectively and to provide corporate support services. If used inappropriately, the same technology and resources may pose significant risks to PHC, its Staff, patients, residents, tenants and clients and to the security of the Information Technology.

1.1. Purpose

The purpose of this Acceptable Use of Information Technology Policy (the "Policy") is to define acceptable conduct and practices for all Users of Information Technology in order to:

- Ensure that the use of Information Technology is consistent with the PHC mission and values
- Ensure that the use of Information Technology complies with professional and ethical obligations and provincial and federal laws
- Protect PHC, its Staff, patients residents, tenants and clients from illegal, damaging or otherwise unacceptable activities (such as intimidation or harassment)
- Respect individual privacy rights
- Safeguard PHC Information Technology assets

1.2. Scope

This policy applies to all Users and all Information Technology.

1.3. Exceptions

Exceptions to this Policy may be made in extraordinary circumstances for approved business or clinical purposes, subject to approval of the Chief Financial Officer. Where there is significant risk to PHC, exceptions must be approved the Senior Leadership Team. Any exceptions must comply with applicable law.

2. Policy

2.1. Ownership of Technology and Records

Information Technology and records generated, handled and stored by Information Technology (including duplicate or back-up copies) are the property of PHC or, as applicable, VCH and/or PHSA in respect of shared systems, except as specifically agreed upon in writing with Staff, or as set out in approved PHC intellectual property policies or third party agreements. In particular, PHC may have agreements with other organizations, such as the University of British Columbia (UBC), which provide that the intellectual property policies of that organization will apply to certain Staff unless there is agreement to the contrary. All messages (including e-mail) generated on or handled by Information Technology are the property of PHC.

2.2. User Authorization

Before using any Information Technology, Users must obtain authorization from the appropriate PHC Manager or representative for the Information Technology required. Users may not access or use Information Technology unless explicitly authorized by PHC.

2.3. Authorized Purpose

Users may only use Information Technology for authorized purposes in accordance with sections 2.4 and 2.5 of this Policy.

2.4. Business/Work Related Purposes

Information Technology may only be used for:

- the performance of job duties and legitimate PHC business purposes; and
- incidental personal use, provided it does not violate the employment obligations of the member of Staff and complies with section 2.5 “Personal Purposes”.

2.5. Personal Purposes

Information Technology may be used for limited, incidental personal purposes provided the following conditions are met:

- use must be infrequent and of short duration, be reasonable and conform to commonly accepted standards of workplace, professional and ethical behavior;
- use is permitted by the individual’s manager or supervisor and does not detract from the User’s performance of his or her job duties;
- use does not compromise the performance of Information Technology or related services;
- use does not impede or adversely affect PHC administrative and business processes;
- use does not compromise the integrity or security of Information Technology;
- use does not expose PHC to costs or risk;
- use is not part of an activity which the User does for personal profit;
- User complies with any specific prohibitions of use of Information Technology established by PHC policies; and
- use otherwise complies with the rest of this Policy and related policies and guidelines, including the Internet Access Policy.

2.6. Terms of Use and System User Guides

Users must comply with any Terms of Use or User Agreements applicable to Information Technology that they have been authorized to use. Users must also comply with any user guides, manuals, instructions or training materials that provide guidance on the proper usage of Information Technology.

2.7. Representation of PHC

All external representations made on behalf of PHC or public disclosure of information concerning PHC via the Internet must be approved by PHC Communications Department and

as necessary, the Information Access and Privacy Office.. This includes, but is not limited to, information such as financial performance, information relating to staff or medical staff, facilities and others. Making fraudulent offers of services, products, items, Information Technology or other PHC assets is prohibited.

2.8. Copyright and Other Intellectual Property Rights

Users of Information Technology must respect and comply with all copyright, patent, trade-mark and any other intellectual property restrictions and conditions contained in applicable product purchase, service or licensing agreements.

2.9. Information Privacy

Staff must ensure that they protect Personal Information when using Information Technology in compliance with the PHC Information Privacy and Confidentiality Policy and related privacy policies.

2.10. Security

Security is the responsibility of every User. The security of Information Technology depends on the appropriate use of these resources.

Users must:

- take all reasonable steps to ensure that Confidential Information and Personal Information is protected from unauthorized use or disclosure. Users are expected to read and understand the IMITS User Security Guidelines (see Appendix B);
- use security controls appropriately, including User IDs and passwords, cable locks, anti-virus software and following security policies; and
- take all reasonable steps to ensure that any PHC Information Technology device assigned to them such as a computer, laptop or other mobile device, is protected from potential theft or loss at all times.

2.11. Prohibited Activities

Users may not use Information Technology or information in a manner that violates PHC policies, ethical obligations or the law. Prohibited activities are set out in the IMITS List of Prohibited Activities (See Appendix A). Users are expected to read and understand the Prohibited Activities List.

2.12. Monitoring and Compliance

Users should not expect privacy when using Information Technology, which may be monitored by PHC in accordance with this Policy. However, PHC recognizes that its right to monitor Information Technology is not absolute. PHC monitors activities appropriate to risks and conducts monitoring in a reasonable manner.

PHC may employ various technologies to enable monitoring of activities. IMITS Security Services shall consult with the Information Access and Privacy Office with respect to the nature of the technologies and proposed use to ensure compliance with applicable privacy

laws and standards. PHC shall implement policies, guidelines and procedures with respect to monitoring, related data storage and retention.

2.13. Purposes of Monitoring

Subject to section 2.12, PHC may, with or without prior notice to Users, examine and filter hard drives, electronic mail messages, web browser cache files, web browser bookmarks, network transmissions, and other information stored on or transmitted through Information Technology for the purposes of:

- investigation of an actual or suspected breach of PHC policies;
- monitoring compliance with this Policy and related policies; or
- monitoring use and performance of Information Technology.

Designated Staff from IMITS Security Services, Information Access & Privacy Office and Human Resources may review audit logs and other records on Information Technology systems on a need to know basis for these purposes.

2.14. Reporting Violations

Users must report any observed or suspected inappropriate use of Information Technology or information to the IMITS Security Services, and in cases where Personal Information may be involved, to the PHC Information Access & Privacy Office, as per the Reporting and Management of Information Privacy Breaches Policy. Where possible, PHC will keep the identity of the individual reporting and the report strictly confidential.

Unless there is immediate risk to PHC, its Staff, patients, residents, tenants or clients, the User's manager or supervisor must authorize the investigation into an actual or suspected misuse of Information Technology before it proceeds.

3. Responsibilities

This section is required, unless procedures have been provided already specifying responsibilities of staff members. List various groups (e.g. management, staff, and specific departments) and describe their responsibilities and activities in enabling the policy. Consider who is responsible for updating, implementing and monitoring or enforcing the policy. Use "will" or "are" statements.

3.1 Information Management Information Technology Services (IMITS)

- Maintain and administer this Policy;
- implement safeguards to protect Information Technology from accidental or intentional misuse;
- provide cost-effective monitoring and compliance mechanisms in support of this Policy;
- develop additional guidelines for permitted and prohibited practices under this Policy; and
- audit and monitor use of Information Technology.

3.2 Information Access & Privacy Office (IAPO)

- Provide guidance on privacy requirements for system access; and
- support IMITS and HR with investigations into non-compliance with this Policy.

3.3 Leaders/Managers/Department Heads

- Ensure that access to Information Technology is provided to Users only as required for job responsibilities; and
- ensure that use of Information Technology complies with this Policy.

3.4 Staff

- Ensure their use of Information Technology complies with this Policy.

4. Compliance

Failure to comply with this policy may result in disciplinary action including, but not limited to, the termination of employment, loss of privileges as a student or volunteer role, prosecution and restitution for damages

5. Supporting Documents

5.1 Related Policies

- Emailing
- Information Privacy and Confidentiality
- Reporting and Management of Privacy Breaches
- Mobile computing & Portable Storage Device Security

6. Definitions

"Information Technology" means computer hardware and software and other technology used in the storage, processing, management and communication of information including, but not limited to, desktop and laptop computers, servers, the VCH/PHC/PHSA network, clinical information systems, electronic mail and messaging, the Internet, the Intranet, voice mail, printers, facsimiles (fax), photocopiers, scanners, telephones, cellular phones, video conferencing equipment, video cameras, digital cameras, hard drives, USB flash memory sticks and other portable storage devices owned, leased, licensed or controlled by PHC/VCH/PHSA.

"Confidential Information" includes information and data, in any form or medium, relating to PHC, its business, operations, activities, planning, personnel, labour relations, suppliers and finances that is not generally available to the public and information that is identified as Confidential Information in accordance with PHC policies.

"IMITS" means the PHSA Information Management Information Technology Services .

"**Personal Information**" means any recorded information about an identifiable individual (including, but not limited to patients, residents, tenants, volunteers, students, staff, physicians or members of the

public), but it does not include business contact information (business contact information is information such as a person's title, business telephone number, business address, email or facsimile number).

"PHC" means Providence Health Care Society

"Staff" means all employees (including management and leadership), medical staff members (including physicians, midwives, dentists) and nurse practitioners, residents, fellows and trainees, health care professionals, students, volunteers, contractors, researchers and other service providers engaged by PHC.
"Terms of Use" (otherwise referred to as "User Agreements") means the terms of use applicable to use of Information Technology systems, which may be in online or paper format.

"User" means any Staff or individual who has been authorized for access to and use of a System.

"VCH" means Vancouver Coastal Health Authority

7. References

BC Freedom of Information and Protection of Privacy Act

8. Appendices

Appendix A: IMITS List of Prohibited Activities

Appendix B: IMITS Security User Guidelines

Appendix A: IMITS List of Prohibited Activities

Prohibited activities using Information Technology include, but are not limited to, the following activities:

1. *Illegal Use*

   Using Information Technology to create or transmit any material (by email, uploading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable local, provincial, national or international law is prohibited.

2. *Threats*

   Using Information Technology or assets to create or transmit any material (by email, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property is prohibited.

3. *Misrepresentation of VCH/PHC*

   Using Information Technology in a manner that misrepresents or may misrepresent the views, services or policies of VCH or PHC is prohibited. All communications purporting to represent the views or policies of VCH or PHC to the public must be pre-approved by PHC Communications and Public Affairs. Unless it is a part of normal job duties, making statements or representations, express or implied, about PHC or VCH/PHC services is prohibited unless authorized by PHC.

4. *Unauthorized Disclosure*

   Using Information Technology in a manner that results in or is likely to result in the unauthorized disclosure of Confidential Information is prohibited.

5. *Cause Harm*

   Users must not use Information Technology in a reckless or other manner that is intended or is likely to cause harm to Staff, patients, residents or others or to VCH or PHC property.

6. *Offensive Material*

   Using Information Technology to view, print, transmit, or create any offensive material including pornography; hate literature or any material that contravenes the PHC Respectful Workplace & Human Rights Policy is prohibited.

7. *Harassment*

   Using Information Technology or assets to create or transmit any material (by email, uploading, posting, or otherwise) that harasses another person is prohibited.

8. *Fraudulent and Unauthorized Commercial Activity*

   Using Information Technology or assets to make fraudulent offers or otherwise conducting unauthorized commercial activity in relation to selling or buying products, items, or Information Technology or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.

9. *Forgery or impersonation*

   Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other

identifying information or using another person's email or other account to send messages or conduct activities without proper authorization is prohibited.

10. *Unsolicited email/Unsolicited bulk email (SPAM)*

    Using Information Technology to create or transmit any unsolicited commercial email or unsolicited bulk email is prohibited. Activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk email, whether or not that email is commercial in nature, are prohibited.

11. *Unauthorized access*

    Using Information Technology to access, or to attempt to access, the accounts of others, or to circumvent, or attempt to circumvent, security measures of PHC's or another entity's information or communications system is prohibited,

12. *Collection of Personal Information*

    Using Information Technology or assets to collect Personal Information without their knowledge or consent is prohibited, unless authorized by applicable laws and PHC policies.

13. *Reselling Information Technology*

    Reselling Information Technology, assets or services without PHC's authorization is prohibited.

14. *Unauthorized Software and Media*

    Installing any non-standard VCH/PHC software, including copyrighted software for which VCH/PHC does not have an active license, is strictly prohibited. The downloading or storage of non-business related media (including movies, MP3's, image files) onto VCH/PHC technology and equipment is prohibited.

15. *Disruptive and Unauthorized System or Network Activities*

    (a) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

    (b) Causing security breaches or disruptions of network communication is prohibited. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

    (c) Port scanning or security scanning is expressly prohibited unless authorized by IMITS Security Services.

    (d) Executing any form of network monitoring which will intercept data not intended for the Staff member is prohibited, unless this activity is a part of the employee's normal job/duty.

    (e) Circumventing user authentication or security of any host, network or account is prohibited.

    (f) Interfering with or denying service, without proper authorization, to any user is prohibited.

(g) Using any program/script/command or sending messages of any kind with the intent to interfere with or disable computer use via any means, without proper authorization, is prohibited.

Appendix B: IMITS User Security Guidelines

Effective security is the responsibility of all PHC staff and other users. This guideline is designed to raise security awareness and enable staff and others to achieve security best practices. It is not intended to cover all aspects of Information Technology security, which are discussed in more detail in PHC security policies.

PHC believes that security is the responsibility of all Staff and other users of Information Technology. The security of Information Technology depends on the proper use of those resources. Security and other technologies may help to protect PHC resources and enforce company policies, but they will have little value if users are not aware of security best practices or attempt to circumvent them, whether intentionally or otherwise. For this reason, PHC strongly emphasizes the need for effective security practices by all individuals who are authorized to access its systems and resources, including Staff, partners and third-party service providers.

Recognize the importance of physical security:

PHC has clearly defined physical security controls in place at all PHC premises. Be aware of the controls and ensure that they remain intact. For example, do not block doors so that they remain open to the outside, and do not admit any unknown person to the premises without properly verifying his or her identity.

Be aware of your surroundings and the activity around you:

Many individuals (including employees, partners and third-party providers) are likely to be performing work on PHC premises at any given time. Some of these people are authorized to have access to sensitive systems and resources, or to specific areas of the premises, while others are not. If you believe someone is working in an inappropriate area or with an inappropriate resource — whether PHC staff or an outside party — you must inform your manager or supervisor.

Be on guard against "social engineering":

Technical security measures are improving rapidly, and for this reason, “social engineering” (fraudulent attempts to gain access to systems or information, often by telephone or e-mail) is becoming commonplace. For example: an unauthorized person may call, pretending to be a company employee who is experiencing a system failure and asking you to give a password or run a specific program. A request of this type is almost certainly fraudulent. Make certain that you know who you are talking to, and if you are in any doubt, contact IMITS Security Services.

Ensure that system maintenance is performed by authorized personnel only:

Maintenance personnel (either internal staff or third-party providers) may sometimes need privileged access to your systems or information resources. In most cases, you will be informed beforehand. If you are in any doubt about a request to access your system, contact your manager or the Service Desk. Do not disclose your password to maintenance personnel under any circumstances.

Rely on VCH/PHC's IMITS personnel for service and support:

While it is often more convenient to ask your colleague next door, only the IMITS Staff is authorized and has the expertise to manage error correction and system configuration consistently throughout the organization. This also applies to software installations and workstation configurations.

Handle passwords with care:

Passwords are the most immediate and visible security measure, and you should handle them with at least the same care you would take with the keys to your home). Do not write them down — and certainly do not hide them under your keyboard or stick them on your monitor — and do not share them with anyone, even your closest colleagues. If you have any suspicion at all that your password may have become known to another person, change it immediately .

Criticize security procedures if necessary, but do not circumvent them:

PHC recognizes that security controls may affect Staff's ability to do their jobs efficiently. If you believe that some security measures are too restrictive, discuss the issue with your manager or with IMITS Security Services. Do not simply try to circumvent the security measures that are causing problems for you.

Handle Confidential Information with due care at all times:

PHC's Confidential Information should be handled appropriately throughout the entire communications chain. For example, confidential documents should be printed only using printers that are in a physically secured location, printouts should be collected immediately, printed documents should be stored in locked cabinets, and documents that are no longer needed should be destroyed.

Follow the Rules in the IMITS List of Prohibited Activities (see Appendix I):

Adhere to the rules prohibiting inappropriate activities using Information Technology as set out in the IMITS List of Prohibited Activities.

Ensure you are familiar with PHC policies:

Security threats are changing rapidly, and so are the measures PHC takes to combat them. For this reason, employees must exercise common sense and keep up to date with PHC's policies and procedures as they evolve to address new risks.

When in doubt, ask:

Effective security depends not only on technical, administrative and legal controls, but also on communication. If you have any questions or concerns about PHC's security policies, do not hesitate to contact your manager, the help desk or IMITS Security Services.

Effective Date:	01-Nov-2013		
First Released:	01-Nov-2013		
Last Revised:	01-Oct-2022 (Minor)		
Last Reviewed:	01-Oct-2022		
Approved By:	PHC	PHSA	VCH
	Shaf Hussain		
Owners:	PHC	PHSA	VCH

Revision History: *(optional)*	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
		Oct 1, 2022	Minor changes	Janet Scott