Policy Title:	Policy Owner: CHIEF INFORMATION OFFICER	
Acceptable Use of Information Technology Resources	Approval by: PRIVACY OFFICER CHIEF INFORMATION OFFICER	
	Original Date	**Revision Date**
	December 8, 2011	**June 6, 2019**
Key Words: Pornography, inappropriate, surfing, computers, responsibility, e-mail, password, acceptable, use, information technology, resources, security, accessing, deleting, copying, printing, disclosing, transmitting, tampering, authorization. Smartphone, sound recordings, video, consent, instant messaging, streaming services, collaboration tools		

POLICY

Information Technology (IT) resources are corporate resources owned by St. Thomas Elgin General Hospital (STEGH). The purpose of this policy is to detail the acceptable use of Information Technology resources (e.g. email, internet access, software applications) which are made available to staff and affiliates to conduct the business of the organization (i.e. for patient care, research, educational and administrative purposes). This policy clarifies STEGH's position regarding the use of IT resources for corporate and personal use.

This policy refers to all IT resources, including all computer and communications equipment installed on STEGH property or otherwise furnished by STEGH, whether individually controlled or shared, stand-alone, or networked. Additionally, this policy highlights the use of social media, including both STEGH-hosted social media and non-STEGH social media in which the person's affiliation with STEGH is known.

Users of IT resources are responsible for:

- Compliance with applicable organization policies and procedures, agreements, guidelines, and legal requirements;
- All activities performed under their user identification (ID);
- The management of their ID and password.

As the owner of IT resources, STEGH reserves the right to audit and monitor these systems' usage and content. This auditing may be conducted, without prior notice, for security reasons, to support ongoing operations, maintenance and upgrades to technology resources, and to support approved investigative activities related to unacceptable use or legal issues.

When devices that are the property of the user are used to access the organization's IT resources, the user must comply with this policy and other STEGH policies and agreements, including the *Bring Your Own Device (BYOD) Policy*.

Personal use of IT resources for functions outside an individual's role should be minimized and should not interfere with the operations and/or policies of the program or organization; and the use must be acceptable.

Social media may be used by all persons for business-related purposes, with only official spokespersons on behalf of STEGH are the President or CEO or delegate and Chair of the Board

of Directors. It is important to remember that online identities and actions are visible to the public, widely accessible, and available for a long time.

1.0 Use of Information Technology Resources

1.1 Acceptable use includes, but is not limited to:

- Use of a strong password;
- Access only those systems to which you have legitimate, authorized access;
- Ongoing vigilance in protecting patient and corporate information through the use of appropriate security practices;
- Use of tools and equipment for the purpose in supporting STEGH operations; and
- Compliance with STEGH's *Social Media Policy* for STEGH-hosted and non-STEGH-hosted social media sites.

1.2 Unacceptable use includes, but is not limited to:

- Sharing of user login ID's and passwords;
- Accessing electronic records of patients or employees where access is not required to perform the duties for which an individual is employed by or affiliated with the organization, including the user's own records and those of family and friends;
- Posting disrespectful, disparaging, insulting, demeaning, sexual, or abusive comments about the Hospital, Employees, Patients, Professional Staff, Volunteers, Board Members, Students, Visitors, or others on social media websites;
- Posting confidential patient information on social media websites;
- Transmission of confidential, business, or patient related information to external sites or servers that are not secure;
- Accessing, modifying, deleting, copying, printing, disclosing, transmitting, or otherwise tampering with files and/or data to which the user has not been provided authorization to access;
- Usage that:
    - Disrupts the operation;
    - Impacts security;
    - Consumes excessive network storage space of IT resources;
- Accessing, uploading, downloading, transmitting, displaying, or distributing obscene or sexually explicit material; transmitting obscene, abusive, or sexually explicit language;
- Providing information about, or lists of, STEGH employees or affiliates to parties outside of STEGH unless approved by Human Resources or Medical Affairs;
- Sending or arranging to receive e-mail in a manner that violates hospital policies or legislation (i.e. Harassment, Ontario Human Rights Code);
- Knowingly introducing malicious programs into the network, servers, or computers (i.e. viruses, worms, Trojan horses, e-mail bombs);
- Installing of any software for which STEGH or the end user does not have an active license;
- Deliberate use of chain messages;
- Making unauthorized copies of or modifying proprietary software or copyrighted material including, but not limited to, music, digitization, and distribution of photographs from magazines, books, or other copyrighted sources;

- Offering unauthorized copies of proprietary software or copyrighted material to others;
- Using IT resources for a criminal act;
- Using hospital computer resources to run or support a private business;
- Removing or altering anti-virus software, update management programs, security or operating system updates/patches from workstations;
- Committing unauthorized electronic entry to, or the circumvention of protective security measures to, an external or internal computer systems or IT resources for 'hacking' type purposes; and
- Ensuring to lock (or "tap out of") one's computer or workstation when leaving the device unattended, while still logged on.

1.3 Staff and affiliates are required to report unacceptable use of IT resources to the individual's Leader, or to the Information Technology Services (ITS) Help Desk.

1.4 Unacceptable use of IT resources may result in discontinuation of network privileges and/or disciplinary action up to and including termination of employment, contract or loss of privileges, or affiliation with the organization, as applicable.

2.0 Electronic Mail and Electronic Messaging System Use

2.1 The St. Thomas Elgin General Hospital's e-mail system and electronic messaging system (e.g. Cisco, Jabber, Blackberry Messaging [BBM]) are:

- A corporate communication tool;
- To be used to conduct the business of the organization; and
- The property of the organization, as well as all data created and stored on its technology

2.2 The organization reserves the right to access an e-mail account in the case of concerns regarding compliance with corporate policies and standards. An e-mail account can only be accessed on the authority of the individual's VP, Director, or designate in coordination with Human Resources. E-mail messages are subject to disclosure during litigation proceedings.

2.3 Staff and affiliates must comply with corporate policies and applicable legislation when using e-mail. Inappropriate use includes, but is not limited to:

- Accessing another individual's e-mail without their consent; or
- Creating, sending, or storing e-mail messages or attachments:
  - That contain offensive material that could constitute harassment under STEGH's Code of Conduct and the Human Rights Code;
  - For private or personal for-profit activities;
  - Of a chain letter nature;
  - Of malicious or threatening nature;
  - Involving impersonation of another e-mail user without the original author's approval;
  - That knowingly sends a virus to another user or group of users;
  - That violate the privacy of a patient's, staff's, or affiliate's information;
  - That are sent to the entire organization indiscriminately;
- Auto-forwarding of e-mail to a system outside of the hospital e-mail system.

2.4 Personal use of the e-mail system for functions outside an individual's role

- Should be minimized;
- Should not interfere with the operations and/or policies or of the program or organization;
- Must be acceptable;
- Must comply with this policy;
- Must not be used to run or operate a business that does not relate to a staff or affiliate's clinical, research, academic, or administrative role; and
- The organization has the right to access these messages, if required.

2.5 E-mail is not a secure, private, or confidential mode of information transmission. Confidential or sensitive business, or identifiable patient or staff/affiliate information must not be transmitted by e-mail external to the organization's secure e-mail system.

2.6 A STEGH e-mail account must not be forwarded to a personal e-mail account external to the organization's secure system (i.e. Gmail, Outlook).

2.7 E-mail should not be used as the primary communication tool with a patient. The use of e-mail to communicate with a patient or Substitute Decision Maker is permissible only when the following procedures are adhered to, including obtaining express informed consent. Printouts of e-mail communication that are pertinent to clinical discussions or decisions must be included in the hospital health record. E-mail must never be used to communicate information of a sensitive nature.

2.8 The organization reserves the right to limit the size of e-mail storage used by each individual to ensure efficient use of hospital IT resources.

2.9 Use of the organization's e-mail system constitutes consent to all terms and conditions of this policy.

2.10 Concerns regarding inappropriate use of e-mail should be referred to management of the staff/affiliate who sent the e-mail for follow up.

2.11 Inappropriate use of e-mail may result in discontinuation of e-mail privileges and/or disciplinary action up to and including termination.

2.12 Information Technology Services is responsible for enforcement of this policy. ITS does not intercept e-mail messages on a regular basis, but will act on an issue when authorized

3.0 Cell Phone and Remote Device Use, including Photography, Video, and Sound Recordings

3.1 Expressed written consent must be obtained before any pictures, video, or sound recordings are taken of any patients or visitors at STEGH, as per the Personal Health Information Protection Act, 2004 (PHIPA). Furthermore, consent forms must be kept on the patient record, please see *Cellular Phone, Wireless and Remote Device Technology Policy – Appendix "A".*

3.2 Verbal consent must also be obtained by any staff or affiliate members (physicians, dentists, midwives) in order to take their photographs, video, or sound recordings. Expressed written consent must be obtained if this media is going to be published anywhere and full disclosure regarding the intent of use must accompany consent requirements as per PHIPA. The use of approved wireless technology is allowed within the Hospital where it can make a contribution to the operation of the hospital and the quality of patient care, in keeping with the requirements of this and referenced policies.

3.3 STEGH-provided IT resources are to be used for Hospital business-related purposes only.

3.4 If travelling and planning to use STEGH-provided IT resources (i.e. cellular telephones) for Hospital business-related purposes, contact Help Desk to ensure the appropriate travel package is applied to the device and to ensure that one can access the Hospital systems (i.e. STEGH e-mail) securely.

3.5 If the IT resource is not utilized for Hospital business-related purposes, while the individual is travelling, this person is expected to reimburse STEGH for the costs acquired.

4.0 Incident Response

4.1 The ITS Department will receive, review, and respond to all reports of computer security incidents, and will review any activity including any real or suspected adverse event in relation to the security of computer systems or computer networks.

5.0 Equipment and Resource Inspection

5.1 All devices requiring access to STEGH data and/or networks must be inspected by a STEGH ITS employee. The inspection is intended to verify that the appropriate level of security is in place as well as verify the existence of proper communication equipment, technical settings, hardware compatibility, and anti-virus protection.

5.2 Any equipment deemed insufficient or risky to the network will be denied access until deemed acceptable.

5.3 Any external equipment and network devices not made available for the inspection may be disconnected from the network until proper inspection is completed.

5.4 If any equipment or network device is suspected of endangering network health, performance, or security is subject to immediate disconnection.

DEFINITIONS

Affiliates:
Individuals not employed by the organization but perform specific tasks at or for the organization, including:

- Physicians, dentists, midwives, extended class nurses;

- Students;
- Volunteers;
- Contractors or contractors' employees who may be members of a third-party contract or under direct contract to the organization; and
  Individuals working at the organization, but funded through an external source (e.g. research employees funded by a university or college).

Confidential:
As per the STEGH *Confidentiality Policy*, STEGH considers the following types of information to be confidential:

- Identifiable personal information and personal health information regarding patients/clients (hereafter referred to as "patients") and their families;
- Identifiable personal information, personal health information, employment information, and compensation information regarding staff and affiliates; and,
- Information regarding the confidential information of the organization, which is not publicly disclosed by the organization.

Confidential Information of the Organization:
Information regarding the organization's business, which is not publicly disclosed by the organization that individuals may come across during the performance of their roles at the organization that is not generally known by the public. Examples of this would be:

- Legal matters that involve the organization that are not public knowledge;
- Financial information that would not be available in the organization's Annual Report;
- Contractual agreements with research sponsors, vendors, third parties, consultants (many times the confidentiality of this information is written within the contract, e.g. non-disclosure of how much we paid for service patents pending, research and development of new technology and treatments, held through the contractual arrangement by sponsors),
- Information related to intellectual property held by the organization, for example, information directly included in patents or other intellectual property applications, prior to publication of those patents or applications in public format, information related to the organization's information technology security and access to systems, including:
  - Information leading to improper access to the organization's computing resources, both internal and external to the hospital network (e.g. "guest" access to systems, remote access credentials);
  - Information pertaining to negotiated product discounts with partner vendors that is considered confidential and proprietary to the vendor;
  - Hardware and software vendor names for products which may be vulnerable to external access attacks, or products that are part of our security infrastructure.

Criminal Act:
An act or the commission of an act that is forbidden or punishable by law or an action prohibited by law, or a failure to act as required by law.

Electronic Mail (e-mail) System:
A computer application used to create and receive electronic messages, and to transmit electronic messages and any other electronic documents in the form of attachments between individual users and/or groups of users.

E-Mail:
Any or several electronic computer records or messages created, sent, forwarded, replied to,

transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several e-mail systems or services. This definition of e-mail records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries and addresses. E-mail messages may be internal or external to the organization.

FTP (File Transfer Protocol):

A user runs software on their computer to connect to a server on the Internet that allows the downloading and uploading of files.

Information Technology Resources include:

- Computing devices and associated peripherals, communications infrastructure and related equipment, facsimile machines, scanners, copiers, telephones, smartphones, tablets and other mobile devices, voice-enabled communication devices, video equipment, other multimedia devices;
- The network, which is a group of computers and associated devices and systems, connected by communications facilities (both hardware and software) to share information and peripheral devices, such as printers;
- All forms of software purchased with hospital funds

Instant Messaging Programs, Collaboration Tools, and Streaming Services:
Programs used to chat, communicate, share, or collaborate with others externally (outside of the London hospital network) over the Internet e.g. BBM, BOX, DropBox, Facebook, FaceTime, Facebook Messenger, Google Drive, OneDrive, Go To Meeting, HipChat, Instagram, Internet Messenger, Jabber, Periscope, Skype, Slack, Snapchat, Tumblr, Twitter, WhatsApp, Teams, Yammer, Zoom, etc.

Password:
A unique and private series of letters and/or numbers and/or special characters used in conjunction with a User ID that enables a user to access a file, a computer, an application, a web page, or a network. Passwords are to be treated as private and confidential*; they are not to be shared*. A password breach could result in possible damage to hospital resources, data and a breach of confidentiality and patient privacy.

Social Media:
Any facility that allows for online publication, commentary and social networking, including but not limited to websites, online forums, blogs, wikis, Facebook, LinkedIn, Tumblr, , Instagram, Twitter, Flickr, Skype and YouTube, etc.

- **STEGH hosted social media**: This refers to corporate social media sites that are created, branded and utilized by STEGH for official hospital purposes. These sites are administered through the Communications Office and Executive Office.
- **Non-STEGH hosted social media**: This refers to social media sties used exclusively for personal purposes. While use of non-STEGH social media sites for educational and personal/professional development is permitted, all use must comply with this policy.

Strong Password:
STEGH has implemented a “strong password” policy. In order for your password to be compliant with this policy, it must contain three of the four following conditions, and it must be at least eight (8) characters in length.

1. At least 1 capital letter

2. At least 1 lowercase letter
3. At least 1 number
4. At least one special character (example: @, $, #, !)

Transmission:
The sending of files, images, data or other information using electronic means such as e-mail, FTP, instant messaging, streaming services (e.g. Facebook Live), or chat programs.

User ID (User Identification):
The short and cryptic name that identifies a user on a computer system. User IDs are unique on a given computer system, i.e. no two users can have the same user ID. Also known as usernames or account names, they could be a combination of your first name, last name, numbers or numbers and letters.

REFERENCES

Bring Your Own Device (BYOD) Policy (STEGH)
Code of Conduct Policy (STEGH)
Confidentiality Policy (STEGH)
Mobile Device Acceptable Use Policy (North Bay Regional Health Centre)
Password Policy (STEGH)
Privacy Policy (STEGH)
Remote Access Policy (STEGH)
Social Media Policy (STEGH) - added