AMGH

Policies & Codes for New Employees

Our Mission

You can count on me

Our Vision

New Horizons for Health and Wellness

Our Values

Innovation
Compassion
Accountability
Respect
Excellence

120 Napier St, Goderich, ON N7A 1W5 519-524-8323 www.amgh.ca

The following book holds the AMGH Policies and Codes that need to be reviewed by every new employee. Once reviewed and by signing and returning your "Offer Letter" you have agreed to adhere to all items.

Note: The links within the policies will take you to our internet site that will not work on the public website.

Policies to be reviewed by everyone:

- Acceptable use of Information, Technology and Resources Agreement Form
- Computer and IT Resources-Acceptable Use (Code of Behavior) Policy
- Confidentiality
- Document Management-Documents, Forms & Records Policy
- Dress Code Policy
- Email Use Policy
- Harassment Policy
- Privacy System Access-EPR Network and PACS Network Policy
- Privacy-General Guidelines
- Respect in the Workplace Policy
- Security Policy
- Social Media Policy
- Violence Prevention in the Workplace Policy

ALEXANDRA MARINE & GENERAL HOSPITAL
120 Napier Street, Goderich, Ontario N7A 1W5
Phone: 519 524 8323; Fax: 519 524 8504

Acceptable Use of Information Technology Resources Agreement

- I have read the Alexandra Marine and General Hospital's Acceptable Use of Information Technology Resources and the E-mail, policy. I will adhere to all related policies and procedures regarding confidentiality, use if information technology, network resources including the Internet, e-mail and other related activities involving hospital computing and privacy.
- I will protect my Password and User ID (hereafter referred to as "access codes") from use by others and will not attempt to use the access codes of others;
- I understand that I am accountable for, and accept responsibility for, all activities carried out under my access codes;
- I will report to Management or Information Systems immediately if I have reason to believe my User ID and/or Password were revealed or compromised;
- I accept responsibility for the accuracy and appropriateness of data that I enter into the organization's patient-care systems;
- I understand that I am required to log off patient-care systems when I have completed my task and that I should not leave an open access unattended;
- I will only access information required to provide care to patients or as directly required in the performance of my duties. If I have more than one User ID, I understand that any given time, I must only use the User ID specific to the role and function that I am performing;
- I will respect the confidentiality and privacy of individuals to whose records I have been given access in compliance with the requirements of the Ontario Personal Health Information Protection Act;
- I have completed, or agree to complete, any training requirements related to my access to the patient-care systems at the hospital; and
- I have read, understand and accept the above statements. I understand that failure to comply with these statements may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the organization.

Alexandra Marine & General Hospital	Information Technology Manual	Initial Live Date: September-28-2012
Approved by: Corporate Leadership	Acceptable Use (Code of Behaviour) of Computer and IT Resources - POLICY	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Policy

User Responsibilities

Information Technology Resources are corporate resources owned by Alexandra Marine and General Hospital. These resources are made available to staff and affiliates to conduct the business of the organization, (i.e., for patient care, research, educational and administrative purposes).

Users of Information Technology Resources are responsible for:

- compliance with applicable organization policies, agreements, guidelines and legal requirements;
- all activities performed under their user identification (ID); and
- the management and security of their ID and password

As the owner of Information Technology Resources, (AMGH) reserves the right to audit and monitor these systems' usage and content. This may be carried out, 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 Information Technology Resources, the user must comply with this policy and other (AMGH) policies and agreements.

Personal use of Information Technology 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.

Staff and affiliates are required to report unacceptable use of Information Technology Resources to the individual's Supervisor and/or to the (Chief Information Officer).

Unacceptable use of Information Technology 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, as determined by AMGH.

Accessing Information

- An individual's e-mail, folder, system, device or other electronic information account may be accessed, reviewed, copied, deleted or disclosed by Information Systems staff and/or the individual's management for reasons that may include:
  - user termination or absence;
  - where there is a reasonable belief that an individual is engaged in inappropriate use of the e-mail system;
  - disclosure to others, including courts and law enforcement agencies, as required by law; and
  - to facilitate the functioning of the e-mail system. Examples of reasons for accessing include;
    - to disable an inappropriately made rule; and
    - to investigate an account that exceeds storage limits that is affecting functioning of the e-mail system for the purpose of maintaining the stability of the e-mail system.

- As part of a random audit
- As deemed necessary by the Chief Information Officer

- Management requesting access to an individual's e-mail account must submit a request via e-mail to the Chief Information Officer with the access reason. Details of the request must include:
  - the name of the account that is to be accessed;
  - the name of the person who will be accessing the account;
  - the reason for access;
  - the length of time in order to provide an audit of this activity; and
  - as part of a random audit.

- The Chief Information Officer may access, review, copy, delete or disclose information from any user in the course of his/her duties (examples: audit, review of resources, investigate issues, terminations, facilitate transfer of information).

Compliance

- Inappropriate use of Computing/Electronic Resources, e-mail and/or MOX is a breach of this policy and may result in disciplinary action by the hospital up to and including termination of employment with cause and/or affiliation with AMGH and/or legal action.

Confidentiality

- Users should take particular caution when circulating and/or printing confidential information via e-mail/MOX.
- Distribution groups should be used to target the appropriate audience for confidential information.
- Users should be aware that, in addition to being subject to authorized access, e-mail/MOX, in its present form, cannot be secured and is therefore vulnerable to unauthorized access and modification by third parties.
- Breaches can be as accidental as selecting the wrong contact in the "TO:" field or breaches can be intentional. Each user should be aware that information stored on a server or published in an e-mail/MOX could be intercepted, purposely or accidentally.
- A statement of confidentiality is appended to all external e-mail.

Copyrights and License Agreements

- It is Alexandra Marine and General Hospital's policy to comply with all laws regarding intellectual property.
- Employees, physicians and volunteers using the Internet are not permitted to copy, transfer, rename, add or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the hospital and or legal action by the copyright owner.

Copyright & License Agreements Employee, Physician and Volunteer Responsibilities

- Employees, physicians and volunteers shall not:
  - Install software unless authorized by IS Support. Only software that is licensed to or owned by Alexandra Marine and General Hospital is to be installed on Alexandra Marine and General Hospital computers.
  - Copy software unless authorized by Alexandra Marine and General Hospital IS Support.
  - Download software unless authorized by Alexandra Marine and General Hospital IS Support.
  - Information Technology will determine in collaboration with the appropriate Director, what software and programs are required on each piece of equipment. Any unauthorized software will be removed by IS Support.

- If such activities listed above do corrupt the integrity of AMGH's IT system (including computers, network and software), the hospital is completely within its right to recover all associated costs if activities are not in keeping with hospital policy.

Copyright & License Agreements IT Support Responsibilities

- Maintain records of software licenses owned by Hospital Name.
- Periodically (at least annually) scan hospital computers to verify that only authorized software is installed. Unauthorized software will be removed by IS support.

Downloads

- File downloads from the Internet are restricted to those that comprise a normal part of hospital business, e.g., Ministry of Health and Long Term Care - Ontario Hospital Reporting System - Hospital Indicator Tool. Authorized downloads should be scheduled in the off hours when possible.

General Computer Use

It is vital that each of us understand that an individual's use of the Hospital computers may affect the overall integrity of the entire Computer Network System.
To this end, all employees must adhere to the following:

- Only log onto appropriate websites;
- Do not log on and remain logged onto the Web or Outlook all day if you are not at your terminal.
- Do not access remote "free services" (e.g. Hotmail, MSN, MySpace, etc.);
- Only open email from known sources. Auto-open routine should not be used;
- Consult with IT Support before downloading software from the Internet, CD or Diskette or other storage media;
- Consult with IT Support before changing computer settings; and
- Do not log onto Radio Stations.

Legal Reference

- Alexandra Marine and General Hospital and its employees, physicians and volunteers are legally bound to comply with the Federal Copyright Act and all proprietary software license agreements.
- This directive applies to all software that is owned by Alexandra Marine and General Hospital, licensed to Alexandra Marine and General Hospital, or developed using Alexandra Marine and General Hospital resources by employees, physicians and volunteers or vendors.

Monitoring Use and Disclosure

- Communication systems and data are the property of AMGH.
- AMGH reserves the right, at its sole discretion and without any further notice, to intercept, retrieve, access, review, archive, destroy, and disclose to others (including courts and law enforcement authorities), all communication systems data and users, including e-mail/MOX and information stored on computers.
- AMGH reserves the right to limit the size of e-mail storage and transmission for all accounts.
- Use of the communication systems constitutes an irrevocable consent to the monitoring and disclosure of system use and data and an agreement to comply with other aspects of this policy.
- All messages created, sent, or retrieved over the Internet are the property of the hospital and may be regarded as public information.
- Alexandra Marine and General Hospital reserves the right to access the contents of any messages, folders, or devices over its facilities if the hospital believes, in its sole judgment, that is has a business need to do so.
- All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Multimedia

- Photographs and videos of staff, collectively or individually, may be taken and utilized by the hospital. Examples of hospital use include, but are not limited to:
  - Bulletin board displays
  - Articles in newspapers
  - Information sessions
  - Website
  - Publications
  - Television
  - Security Camera
- A staff member who wishes to limit the use of the above must notify the Chief Information Officer in writing of such for consideration.

Outlook and Meditech Distribution Groups Use - "All User" Messages - Meditech and Outlook

- The "All User" or Group distribution lists are used to distribute messages of significant importance to all or a vast majority of AMGH staff and physicians.
- Use of "All User" distribution is limited to administration. It is not appropriate to use the "All User" distribution list for personal use.
- A member of Administration may give a special authorization to utilize "all users", allowing them to present or promote some cultural, sports or fund raising events. Otherwise, each user is responsible for targeting the appropriate audience to a message.
- Specific distribution groups have been set up to assist in appropriately targeting the right audience. These groups can be found within the general address book. To set up additional distribution groups, contact the Information Systems department for assistance.
- All "All Users or Large Group Emails" MUST be approved by your Supervisor PRIOR to sending.
- All "All Users or Large Group Emails" should utilize the "delete on" feature (found under "Special Handling") to ensure that they are automatically deleted once no longer pertinent.

Passwords and Access Codes

- The confidentiality and integrity of data stored on hospital computer systems must be protected by access controls to ensure that only authorized employees, physicians and volunteers have access.
- This access shall be in accordance with defined requirements for each job function as determined by IT Services
- The AMGH Information Systems is responsible for the administration of access controls to all hospital computer systems.
- IT Services will process additions, deletions, and changes upon receipt of the access authorization form, from the end user's direct supervisor.

Passwords and Access Codes Employee Responsibilities

Each Employee:

- Is responsible for all computer transactions that are made with his/her User ID and password including electronic single sign on.
- Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
- Will change passwords as prompted by the information system and as directed.
- Should use passwords that will not be easily guessed by others.
- Should log out when leaving a workstation for an extended period.
- The guidelines for passwords are:
  - Allowable characters are the 26 letters of the alphabet and digits with zero to nine.

- Length of 8 characters minimum ideally.
- Inclusion of at least one number (can be located anywhere in the password beginning, end, or embedded).
- Each password should be individual to the user and difficult to decipher. Avoid use of license plate numbers, children's names, and other word sequences that could be connected to you by others.

Remote Access

- Granted on an as needed basis as identified by immediate supervisor in consultation with consultation with IT.
- Methodology is identified by IS services.
- Reviewed annually by IS services and as required.

Removal of Confidential Information from the Organization Property

Staff and affiliates are responsible to remove confidential information from the organization only if required as part of the role for which he/she has been hired, or affiliated with the organization. Staff or affiliates removing information from the organization are responsible:

- To follow any hospital policies regarding removal and/or handling of confidential information
- to take reasonable steps to ensure the security of the information, regardless of the media;
- to remove only the minimum amount of confidential information necessary, for the minimum time required to accomplish the purpose (i.e., return information to the organization as soon as possible);
- to access confidential information in protected areas (e.g., not in public places where others can view it);
- to never leave confidential information unattended in a motor vehicle;
- if necessary, to retain confidential information in his/her home, to keep it in a secure area, not in view of others; and
- Supervisors are responsible to be aware of roles within their program(s) where staff and affiliates are required to remove confidential information and to ensure that staff and affiliates are aware of their obligations related to security of the confidential information.

Saving Information

- Patient information should be stored on the network servers, in a password protected folder. This ensures the data can be securely accessed from various locations, is up to date, and is backed up regularly.
- If patient information has to be stored locally, then it must be password protected, and backed up to another medium on a regular basis as appropriate.
- Information should not be stored in "My Documents". Information should be stored in a mapped folder.
- If mobile devices are used for storage of patient and/or corporate information, the mobile device must be encrypted.

Security – IT Support Responsibilities

- Alexandra Marine and General Hospital IM Support team is responsible for all equipment installations, disconnections, modifications, and relocations - employees, physicians and volunteers are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IS.

Security - User Responsibilities

- The directives below apply to all employees, physicians and volunteers:
  - Memory sticks, CDs and storage drives should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up or have encryption installed.

- Length of 8 characters minimum ideally.
- Inclusion of at least one number (can be located anywhere in the password beginning, end, or embedded).
- Each password should be individual to the user and difficult to decipher. Avoid use of license plate numbers, children's names, and other word sequences that could be connected to you by others.

Remote Access

- Granted on an as needed basis as identified by immediate supervisor in consultation with consultation with IT.
- Methodology is identified by IS services.
- Reviewed annually by IS services and as required.

Removal of Confidential Information from the Organization Property

Staff and affiliates are responsible to remove confidential information from the organization only if required as part of the role for which he/she has been hired, or affiliated with the organization. Staff or affiliates removing information from the organization are responsible:

- To follow any hospital policies regarding removal and/or handling of confidential information
- to take reasonable steps to ensure the security of the information, regardless of the media;
- to remove only the minimum amount of confidential information necessary, for the minimum time required to accomplish the purpose (i.e., return information to the organization as soon as possible);
- to access confidential information in protected areas (e.g., not in public places where others can view it);
- to never leave confidential information unattended in a motor vehicle;
- if necessary, to retain confidential information in his/her home, to keep it in a secure area, not in view of others; and
- Supervisors are responsible to be aware of roles within their program(s) where staff and affiliates are required to remove confidential information and to ensure that staff and affiliates are aware of their obligations related to security of the confidential information.

Saving Information

- Patient information should be stored on the network servers, in a password protected folder. This ensures the data can be securely accessed from various locations, is up to date, and is backed up regularly.
- If patient information has to be stored locally, then it must be password protected, and backed up to another medium on a regular basis as appropriate.
- Information should not be stored in "My Documents". Information should be stored in a mapped folder.
- If mobile devices are used for storage of patient and/or corporate information, the mobile device must be encrypted.

Security – IT Support Responsibilities

- Alexandra Marine and General Hospital IM Support team is responsible for all equipment installations, disconnections, modifications, and relocations - employees, physicians and volunteers are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IS.

Security - User Responsibilities

- The directives below apply to all employees, physicians and volunteers:
  - Memory sticks, CDs and storage drives should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up or have encryption installed.

Alexandra Marine & General Hospital	Freedom of Information & Privacy Manual	Initial Live Date: August-26-2012
Approved by: Corporate Leadership	Confidentiality Agreement	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Policy

Alexandra Marine and General Hospital (AMGH) has a legal and ethical responsibility to protect the privacy of patients / residents /clients, their families, and staff / affiliates, and ensure confidentiality is maintained.

AMGH considers the following types of information to be confidential:

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

This policy applies whether this information is verbal, written, electronic, or in any other format. Audits are performed to determine compliance.

In addition to standards of confidentiality, which govern Regulated Health Professionals, staff and affiliates are bound by the organization's responsibility to maintain confidentiality. The organization expects staff / affiliates to keep information, which they may learn or have access to because of their employment/affiliation, in the strictest confidence.

It is the responsibility of every staff/affiliate to:

- Be familiar with and follow the organization's policies and procedures regarding the collection, use, disclosure, storage, and destruction of confidential information; including privacy policies, E-mail policy and release of information policy.
  Refer to:
  - **E-Mail (Electronic Mail) Use Policy**
  - **Privacy Policy**
  - **Release of Information Policy**
- Collect, access, and use confidential information only as authorized and required to provide care or perform their assigned duties;
- Continue to respect and maintain the terms of the Confidentiality Agreement after an individual's employment / affiliation with the organization ends;
- Discuss confidential information only with those who require this information to provide care or perform their duties and make every effort to discuss confidential information out of range of others who should not have access to this information;
- Divulge, copy, transmit, or release confidential information only as authorized and needed to provide care or perform their duties;
- Identify confidential information as such when sending E-mails or fax transmissions and to provide direction to the recipient if they receive a transmission in error;
- Participate in the organization's Privacy and Confidentiality education program, review this policy, and sign a Confidentiality Agreement before commencing work or the provision of service at AMGH as a condition of employment / appointment / contract / association for staff / affiliates at AMGH
- Report to their Supervisor suspected breaches of confidentiality or within the organization that compromise confidential information. If the Leader is the individual suspected of the breach, staff / affiliates may contact Privacy Officer or Human Resources / Chief of Service.
- Safeguard passwords and/or any other user codes that access computer systems and programs.

Misuse, failure to safeguard, or the disclosure of confidential information without appropriate approvals may be cause for disciplinary action up to and including termination of employment / contract or loss of appointment or affiliation with the organization.

Procedure

General

- Supervisors must review any department specific information or procedures related to confidentiality with new staff and affiliates.
- Staff / affiliates may consult their Supervisor, Privacy Officer, Human Resources or Risk Management regarding confidentiality issues or inquiries.

Confidentiality Agreement

- Confirmation of the successful completion of the educational program and the signed Confidentiality Agreement will be kept on the individual's file in:
    - CEO's office for physicians, residents, medical students, dentists, and midwives, secretaries who are privately employed by physicians, Medical Department Administrative Officers;
    - Human Resources for staff;
    - Human Resources for volunteers, contract staff, consultants, and students; and

It is the responsibility of applicable Supervisor and Human Resources to stipulate in Education Affiliation Agreements with education institutions, the obligation to ensure that students and faculty abide by the organization's standards of confidentiality.

Investigating Alleged Breaches of Confidentiality

It is the responsibility of Supervisors in conjunction with Human Resources, Risk Management, and Privacy Officer, to investigate alleged breaches of confidentiality.

Definitions

Affiliates - Individuals who are not employed by the organization but perform specific tasks at or for the organization, including appointed professionals (e.g., physicians / midwives / dentists), students, volunteers, researchers, contractors, or contractor 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.

Confidential Business 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 vendors, third parties, consultants (many times the confidentiality of this information is written within the contract e.g., nondisclosure of how much we paid for service);
- information related to intellectual property, e.g., patents pending, research and development of new technology and treatments; and
- 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; and

- hardware and software vendor names for products which may be vulnerable to external access attacks, or products that are part of our security infrastructure.

Personal Health Information - Personal information with respect to an individual, whether living or deceased and includes:

- information concerning the physical or mental health of the individual;
- information concerning any health service provided to the individual;
- information concerning the donation by the individual of any body part or any bodily substance of the individual;
- information derived from the testing or examination of a body part or bodily substance of the individual;
- information that is collected in the course of providing health services to the individual; or
- information that is collected incidentally to the provision of health services to the individual.

Personal Information - Information about an identifiable individual, but does not include the name, title or business address or business telephone number of staff member of an organization.

Related Information

Statement of Confidentiality

References

- LHSC Confidentiality Policy, Correspondence and Personal Communication; 2008
- Lakeridge Health Confidentiality Agreement, 2012

Alexandra Marine & General Hospital	Administration Manual	Initial Live Date: June-5-2012
Approved by: Corporate Leadership	Document Management - Documents, Forms and Records	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Policy
AMGH has a document and records management system to create, control and maintain all documents and records. It is a web based software program (called DocuShare®) and can be found in the Internet at https://docushare.intranet.amgh.ca/docushare/

This policy provides direction for the processes and procedures for managing the documents and records.

Definitions
Documents: include any information that provides direction (e.g., instructions including forms, textbooks, reference intervals and their origins, specifications, calibration tables, charts, posters, notices, memoranda, plans, software, drawings, regulations and standards).

Records: include any information that produces evidence (e.g., requisitions, examination results and reports, instrument printouts, workbooks and worksheets, accession records, calibration records, quality control records, records of audits, complaints and action taken, external quality assessment records, instrument maintenance records, staff training and competency records, personnel records).

Responsibility
Senior Administration is responsible for reviewing, approving new and changed documents and records, and establishing effective dates and retention times for them (in keeping with Records Retention Policy).

Managers/Directors/Designates are responsible for reviewing, distributing, retaining and notifying staff of new or changed documents and records.

Staff are responsible for reviewing new and changed documents and understanding that the official documents are found in the document control software program and nowhere else.

Document Management Clerks, under the direction of the Chief Information Officer, are responsible for managing the document control system to include (but not limited to): creating and maintaining the Master File, assigning unique identifiers, publishing, routing and archiving documents.

Retention
Documents and records will be held according to hospital policy. Refer to Retention of Records.

Documents storage prevents damage and unauthorized access while facilitating retrieval.

Once the storage time has passed, the documents/records may be destroyed, according to hospital policy.

Alexandra Marine & General Hospital	MANUAL: Human Resources	Revision Date: February-4-2016
Approved by: Corporate Leadership	Dress Code Guidelines	Original Date: November-19-2012

Policy

It is the policy of this hospital to present an image to patients, visitors and the community that is professional and inspires confidence. The overall presentation of staff members is an important contributing factor to this image.

Dress, grooming and conduct must be consistent with the work in our professional work environment, health and safety regulations, infection control guidelines and within the standards determined for optimum patient care. This policy is also to include situations when employees are attending hospital meetings, in-services and/or training sessions, etc.

Principles

1. Employee Safety - employee and patient safety may be compromised by inappropriate or unsafe attire and footwear, unsecured hair and personal adornments, heavy scents and odors etc.
2. Infection Control - uniforms and protective clothing serves the purpose of reducing the possibility of transfer of infectious organisms to patients or into the home of the employee.
3. Professionalism - patient confidence can be affected by the appearance of those who are providing care.
4. Appropriateness - an employee's dress must be appropriate to the activities and responsibilities of their position
    - No low neckline
    - no exposed abdomens or lower backs

General Guidelines

1. Departmental specific dress code guidelines will be in writing and complement this policy as appropriate.
2. All staff must wear their photo identification badge at all times when on duty as per the *Identification Badge Policy*.
3. Uniforms/clothing must be neat, clean and loose enough to permit free movement and of a length that presents a professional image. Shorts, skirts/dresses are to be long enough to extend to within three inches above one's knee.
4. Some departments require more specific dress code standards. These standards are to be outlined in the departmental policy manual and are to be provided at the time of hiring by the individual department. All department specific dress code policies are to be reviewed by the Occupational Health Coordinator.
5. Some departments require the use of protective clothing and personal protective equipment. Please refer to the appropriate Occupational Health Policies and Infection Control Policies. Protective clothing as determined by each department shall be worn as required.
6. All uniforms supplied by the hospital remain the property of the hospital and may be worn only while on duty.
7. Uniforms and clothing must be free of advertisements and slogans.
8. Lanyards, buttons and pins must be plain, AMGH approved items and must be free of advertisements and slogans.
9. All footwear must be safe, clean and in good condition at all times and appropriate to the work environment. All employees are required to wear footwear appropriate for the potential hazards present in their work environment, unless certain footwear is deemed medically necessary.

Supervisors are responsible for ensuring employees wear appropriate footwear. Please refer to the Risk Assessment Chart as your guide.

10. Where infection control is a concern, nail polish is not allowed; otherwise, clear or pastel nail polish is permitted. Nail polish must be in good repair. Staff working in a clinical area or having direct patient contact must not wear artificial or acrylic nails.
11. Hair should be clean and neatly styled. Hair accessories should be limited and appropriate to a professional image. Size and amount of jewelry, including body piercing should be professional in appearance, conservative and safe from an infection control and employee safety standard, and may be restricted depending on the area where the employee works.
12. Fragrance use should be kept to a minimum. Individual departments may elect to be "Scent Reduced" to protect staff/patients from exposure to scent. This will be coordinated with Occupational Health.

Compliance

It is expected that all staff members assume responsibility for their own appearance.
When a Supervisor observes or receives complaints from others regarding the personal appearance of an employee to be considered unsuitable for the workplace, she/he will discuss the matter in private with the employee. Employees who fail to present themselves in accordance with this policy may be subject to corrective action as appropriate.
Repeated non-compliance with the dress code shall result in regular progressive disciplinary procedures.

Risk Assessment Chart

Low to Moderate Risk

a. Potential Hazards
   - Typical office environments
   - Clinics with little risk of splashes of chemical or biological agents and where needles and other sharps are not used
   - Heavy materials, heavy equipment or furniture is not handled or moved - Patient care, employees who work in clinical areas or may enter clinical areas as part of their job function (i.e. - support staff, clinical leaders)
   - Laboratories
   - Where needles or other sharps may be used Where blood or biological fluid splashes may occur
   - Where chemicals are handled in a controlled setting (e.g. Fume hoods)

b. Appropriate Footwear

The foot wear must have the following characteristics:
   - Closed toe and heel (sandals or open-toed shoes are not allowed) - The sole is made of non-slip, shock absorbent materials.
   - The heel is low to moderate.
   - The shoe material must be durable and impermeable to protect from chemicals, hot liquids or sharps such as needles.
   - An example of appropriate footwear is a running/walking shoe
   - Footwear should not be noisy

High Risk

1. Potential Hazards
   - Heavy materials, heavy equipment
   - Maintenance work
   - Moderate to large volumes of hazardous substances
2. Appropriate Footwear
   - Footwear must comply with CSA standards: Example - safety boot

Source

Risk Assessment Chart - Ontario Safety Association for Community and Healthcare

Alexandra Marine & General Hospital	Information Technology Manual	Initial Live Date: September-28-2012
Approved by: Corporate Leadership	Email Use POLICY	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Policy

This policy applies to staff and affiliates who have been given access to the organization's electronic mail (e-mail) system.

The Alexandra Marine and General Hospital (AMGH) e-mail system is:

- 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 this technology.

Use of the organization's e-mail system constitutes consent to all terms and conditions of this policy. It is an expectation and requirement of employment for staff members to check emails routinely, review actions and respond as appropriate in a timely way.

Concerns regarding inappropriate use of e-mail should be referred to management of the staff/affiliate who sent the e-mail for appropriate follow-up. Inappropriate use of e-mail may result in discontinuation of e-mail privileges and/or disciplinary action up to and including termination of employment/contract and/or loss of privileges or affiliation with the organization.

The Chief Information Officer is responsible for enforcement of this policy. CIO does not intercept e-mail messages on a regular basis, but will act on issues as they arise and/or as the need arises and/or randomly through audits.

AMGH reserves the right to audit and monitor e-mail usage and content. All email sent and received by AMGH staff is considered property of AMGH. There is no personal right to privacy in any matter created, received or sent from any portion of AMGH's email system. E-mail messages are not inherently encrypted, therefore there is no guarantee of the confidentiality and security of messages users send to or receive from others; the exception to this is when a user has been authorized for confidential email usage.

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 Director/delegate or the Chief of Staff, as appropriate or on the authority of the Chief Information Officer or through random audits. E-mail messages are subject to disclosure during litigation proceedings.

Email Account Management

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

Outlook and email must not be used as a document management system. Official documents must be retained on the hospital network (my documents), in the document management system or in paper format as per the record retention policy. This includes email messages that are official documents (example: offer letter composed and sent via email or a contract received via email).

Outlook is not used for storing any official documents and, as such, all items in Outlook including emails, tasks, calendar events and notes that are more than 6 months old are automatically deleted on a monthly basis.

Emails, including attachments, must also be dealt with according to their content; and any emails or information contained therein that is subject to a retention period must be handled accordingly and saved by the user on the hospital network (my documents), in the document management system or in paper format as per the record retention policy..

Appropriate Use

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 his or her consent, or
- creating, sending, or storing e-mail messages or attachments:
  - that contain offensive material that could constitute harassment under the AMGH Harassment Policy, and the Ontario Human Rights Code;
  - for private or personal for-profit activities;
  - of a chain letter nature;
  - of a malicious or threatening nature;
  - involving impersonation of another e-mail user;
  - in which the original content has been altered without the original author's approval;
  - that knowingly send a virus to another user or group of users;
  - that violate the privacy of patient, staff or affiliate information; or
  - that are sent to the entire organization indiscriminately.
  - Use of profanity, offensive language regardless of format
- Auto-forwarding of e-mail to a system outside of the hospital e-mail system.

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 of the program or organization;
- should not contain any personal or private information;
- must be acceptable (see Acceptable Use of Information Technology Resources Policy);
- must comply with this policy; and
- must not be used to run or operate a business that does not relate to a staff or affiliates clinical, research academic or administrative role.

The organization has the right to access these messages.

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.

An AMGH e-mail account must not be forwarded to an e-mail account external to the organization's secure system without IT knowledge.

Instant messaging and E-Mail

No public instant messaging service is permitted.

Users must not knowingly open or transmit personal identifiable information or PHSA confidential information over external electronic messaging unless the information has been encrypted and authenticated using AMGH standard encryption software.

Using external email sources such as Hot Mail, Yahoo or other non-AMGH email accounts to access or transmit AMGH data, records or Information is prohibited.

Users must not send or forward chain email, i.e: messages containing instructions to forward the message to others.

Emailing Personal Health information

AMGH users shall never send personal Patient Identifiable information or Personal Health Information (PHI) in any OUTLOOK email without being authorized for confidential email usage. This restriction applies to all OUTLOOK emails sent internally staff to staff, and also to external recipients such as physicians, other non-AMGH care providers, outside vendors, friends, family, etc. AMGH's OUTLOOK email system is not considered an acceptable mode of communication of patient related updates to care providers or patient's family members. Should a staff member feel that using Outlook for communication personal or personal health information is essential, they must follow the "**Procedure for Confidential Email Usage**" outlined below. Any requests to use Outlook for transmitting PHI will be reviewed with the utmost scrutiny and will be authorized only in special cases.

Staff found to have breached this Policy are subject to temporary or permanent loss of access privileges and/or legal sanctions and/or discipline up to and including termination.

The policy applies to:

- All users of the AMGH email system
- Internal and External email usage
- Email usage via Microsoft Outlook (full version) and OWA
- All file/date types within the email system including emails, calendar items, tasks, notes and contacts.

Procedure for Confidential Email Usage:

1. Complete the "Authorization for Confidential Email Usage" form located in Meditech Forms online.
2. Send via email or inter-office mail to CIO
3. Pending authorization, the hospital's IT department will communicate next steps for encrypting email.

- Authorized users should treat confidential information as temporary and should be retained in an e-mail user's account only for as long as is necessary to fulfill the purposes for which it was intended.

Emailing Patient Health Record Numbers

There is the occasion when it is necessary to send a list of Health Record Numbers to another staff / affiliate via email.

1. Send a first email to the address requesting this information. Explain that the requested numbers will arrive in an email to follow.
2. Send a second email with only the 5 or 6 digit health record number/s. Do not include the "G" or "G0" preceding the number. This allows less opportunity to identify a patient in our system.

Canada's Anti-Spam Legislation (CASL)

Canada's Anti-Spam Legislation (CASL) establishes rules for the sending of commercial electronic messages (CEMs) and the installation of computer programs. CEMs can include emails, SMS text messages, instant messages and messages sent through social networks that communicate participation in a commercial activity. This includes advertisements and information about promotions, offers, business opportunities, events, etc. Under CASL, consent is required before sending this type of message. All AMGH end users are to comply with the contents of CASL. Further information can be found at http://fightspam.gc.ca/eic/site/030.nsf/eng/home

Procedures

Distribution Groups

All requests for Distribution Groups are forwarded to the Chief Information Officer. Generally, Distribution Groups are only set up for hospital wide groups and not individual or departmental groups that are not used by all staff.

Users must not sent mass mailing lists e-mails for non-hospital events unless approved by a member of ELT.

Divulging AMGH email addresses or distribution lists for non-business related activities is prohibited.

Electronic mail messages and attachments may be accessible to others under certain circumstances set out under the Freedom of Information and Protection of Privacy Act (FIPPA). The intention alteration or destruction of an electronic message or record for the purpose of evading an access request is an offence under FIPPA.

Accessing an E-mail Account

An individual's e-mail account may be accessed, reviewed, copied, deleted or disclosed by Information Systems Staff/CIO and/or the individual's management for reasons that may include:

- user termination or absence;
- where there is a reasonable belief that an individual is engaged in inappropriate use of the e-mail system;
- disclosure to others, including courts and law enforcement agencies, as required by law; and
- to facilitate the functioning of the e-mail system. Examples of reasons for accessing include;
    - to disable an inappropriately made rule; and
    - to investigate an account that exceeds storage limits that is affecting functioning of the e-mail system for the purpose of maintaining the stability of the e-mail system.
- As part of random audits
- To retrieve information, examples include:
    - FOI requests, search for records/information.

Management requesting access to an individual's e-mail account must submit a request via e-mail to the Chief Information Officer with the access reason. Details of the request must include:

- the name of the account that is to be accessed;
- the name of the person who will be accessing the account;
- the reason for access;
- the length of time in order to provide an audit of this activity; and
- as part of a random audit.

Definitions

Affiliates - individuals who are not employed by the organization but perform specific tasks at or for the organization, including professional with privileges (e.g., physicians), students, volunteers, contractors, or contractor 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 UWO).

Attachments - those documents appended to and transmitted with an e-mail message such as work processing documents, spreadsheets, sound files, image files, hot links, etc.

Confidential - as per the AMGH Confidentiality policy, AMGH considers the following types of information to be confidential:

- personal information and personal health information regarding patients, residents, clients (hereafter referred to as "patients") and their families;
- personal information, personal health information, employment information, and compensation information regarding staff and affiliates; and
- information regarding the organization's operations that is not publicly disclosed by the organization (e.g., unpublished financial statements, legal matters).

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.

Encryption - the process of mathematically scrambling a text message from plain text to cipher text to make it unreadable.

Identifiable Information - for the purpose of this policy, identifiable information means information that:

- identifies the individual by name, address, identifying number (e.g., Health Card #, PIN#)
- could potentially identify the individual if the information is combined with other available information.

Patient - for the purpose of this policy "patient" refers to a patient, resident or client who is an inpatient or outpatient.

Personal Health Information - personal information about an identifiable individual, whether living or deceased and includes:

a. information concerning the physical or mental health of the individual;
b. information concerning any health service provided to the individual;
c. information concerning the donation by the individual of any body part or any bodily substance of the individual;
d. information derived from the testing or examination of a body part or bodily substance of the individual;
e. information that is collected in the course of providing health services to the individual; and
f. information that is collected incidentally to the provision of health services to the individual.

Personal information - information about an identifiable individual, but does not include the name, title or business address or business telephone number of a staff member of an organization. For the purpose of this policy personal information may include name, address, age, financial or legal (Mental Health status) information.

Secure File Transfer System - a web-based application that is used to transfer files to one or a number of recipients securely. It uses 128-bit encryption to protect the transfer of files. This is the same level of encryption used by banks for on-line banking.

Sensitive - for the purpose of this policy, sensitive information may include personal or health information that would be most appropriately delivered in person because the impact of disclosing the information may cause an emotional effect on the individual, or may give someone an advantage if revealed to persons not entitled to know it.

References

LHSC Electronic Mail (E-Mail) Use Policy, Correspondence, and Personal Communication; 2008

Employment Standards in Ontario

The Employment Standards Act, 2000 (ESA) sets minimum standards for most workplaces in Ontario. Special rules and exemptions apply to certain employees.

What you need to know

> Employers are prohibited from penalizing employees in any way for exercising **ESA** rights.

Hours of Work and Eating Periods: There are daily and weekly limits on hours of work. Employees may work more if certain conditions are met. Employees must not work more than 5 consecutive hours without a 30-minute meal break. Learn more at **Ontario.ca/hoursofwork**.

Overtime Pay: Overtime is payable after 44 hours of work in a week for most jobs. The overtime rate must be at least 1½ times the regular rate of pay.

Minimum Wage: Most employees are entitled to be paid at least the minimum wage. For current rates visit **Ontario.ca/minimumwage**.

Payday: Employees must be paid on a regular payday and receive a wage statement.

Vacation Time and Pay: Most employees earn at least 2 weeks of vacation time after every 12 months. They must be paid at least 4% of the total wages they earned as vacation pay.

Public Holidays: Ontario has 9 public holidays each year. Most employees are entitled to take these days off work and be paid public holiday pay.

Leaves of Absence: There are a number of job-protected unpaid leaves of absence including pregnancy, parental, family caregiver, and personal emergency leave.

Termination Notice and Pay: In most cases, employers must give advance written notice when terminating employment and/or termination pay instead of notice. Learn more at **Ontario.ca/terminationofemployment**.

Other ESA Rights and Special Rules: There are other rights as well as special rules not listed on this poster including rights to severance pay and special rules for assignment employees of temporary help agencies.

Contact the Ministry of Labour for more information

Call us at 416-326-7160, 1-800-531-5551, TTY 1-866-567-8893, or visit our website at **Ontario.ca/employmentstandards. Information is available in multiple languages.**

Version 6.0 ©Queen's Printer for Ontario, 2015 Printed in Canada
ISBN 978-1-4606-5184-1 (Print) ISBN 978-1-4606-5185-8 (HTML) ISBN 978-1-4606-5186-5 (PDF)

Ontario

Alexandra Marine & General Hospital	MANUAL: Human Resources	Revision Date: August-11-2016
Approved by: Executive Leadership	Harassment and Discrimination policy	Original Date: November-19-2012

Policy

Alexandra Marine and General Hospital (AMGH) is committed to providing a working environment free of discrimination and harassment, in which all individuals (staff, Physicians, volunteers and visitors) are treated with respect and dignity, can contribute fully and have equal opportunities. Each individual has the right to work in an atmosphere which is fair, equitable and free from all forms of discrimination and harassment. It is each person's responsibility to uphold these beliefs.

The purpose of this policy is to acknowledge that such conduct, contrary to this commitment, is unacceptable and intolerable and will result in disciplinary actions up to and including the termination of employment, with cause. Investigation of any complaints of harassment or discriminations will be initiated within 72 hours.

Purpose

To provide employees with a mechanism to ensure the work place is free from any type of personal harassment or discrimination.

Discrimination: Means any form of unequal treatment based on the Ontario Human Rights Code, whether imposing extra burdens or denying benefits. It may be intentional or unintentional. It may involve direct actions that are discriminatory, or it may involve rules, practices or procedures that appear neutral, but disadvantage certain groups of people. Discrimination may take obvious forms, or may happen in subtle ways. Even if there are many factors affecting a decision or action, if discrimination is one factor that is a violation of this policy.

Harassment: Means any course of comments or actions that are known, or ought reasonably to be known, to be unwelcome. It can involve words or actions that are known or should be known to be offensive, embarrassing, humiliating, demeaning or unwelcome, based on a ground of discrimination identified by this policy. Harassment can occur based on any of the grounds of discrimination.

This policy prohibits discrimination or harassment based on the following grounds, and any combination of these grounds:

- Age
- Creed (religion)
- Sex (including pregnancy and breastfeeding)
- Sexual orientation
- Gender identity
- Gender expression
- Family status (such as being in a parent-child relationship)
- Marital status (including married, single, widowed, divorced, separated or living in a conjugal relationship outside of marriage, whether in a same-sex or opposite-sex relationship)
- Disability (including mental, physical, developmental or learning disabilities)
- Race
- Ancestry
- Place of origin
- Ethnic origin
- Citizenship
- Color

- Record of offences (criminal conviction for a provincial offence, or for an offence for which a pardon has been received)
- Association or relationship with a person identified by one of the above grounds
- Perception that one of the above grounds applies.

Examples of Harassment

Psychological

Harassment in the workplace which creates a poisonous, uncomfortable, unwelcome and offensive work environment - may include intimidation, threats or coercion, exclusion or isolation.

Sexual

Workplace sexual harassment would include harassment of a worker because of sex, sexual orientation, gender identity or gender expression or an unwelcome sexual solicitation or advance by a person who is in the position to confer, grant or deny a benefit or advancement. (Ministry of Labour definition of sexual harassment, 2016)

Personal

Personal harassment consists of unwelcome comments or actions that demean or humiliate an employee. It is objectionable conduct which serves no legitimate work purpose and has the effect of creating an intimidating, humiliating, hostile or negative work environment. Unlike all the other forms of harassment, the comments or actions do not need to be based on any of the protected grounds such as age, sex, or race. Personal harassment is abusive, inappropriate behaviour that is nasty, but not discriminatory.

Poisoned Environment

A poisoned environment is created by comments or conduct (including comments or conduct that are condoned or allowed to continue when brought to the attention of management) that create a discriminatory work environment. The comments or conduct need not be directed at a specific person, and may be from any person, regardless of positon or status. A single comment or action, if sufficiently serious, may create a poisoned environment.

Roles and Responsibilities

All persons present at AMGH are expected to uphold and abide by this policy, by refraining from any form of harassment or discrimination, and by cooperating fully in any investigation of harassment to discrimination complaint.

Managers and supervisors have the additional responsibility to act immediately on observations or allegations of harassment or discrimination. Managers and supervisors are responsible for creating and maintaining a harassment and discrimination free organization, and should address potential problems before they become serious.

Personal Harassment Complaint

Process For Resolution

An individual who believes they are a victim of harassment should take any or all of the following actions as soon as possible.

Make it known to the person subject to the complaint that their behaviour is offensive and unwelcome. There may be situations where a person is unable or unwilling to confront his or her harasser. This does not prevent an individual from making a complaint;

Keep a written record of date(s), time(s), details of incident(s) and witnesses to the incident(s) if any; and

Where a person does not wish to confront the harasser, or where such an approach is attempted and does not produce a satisfactory result, a complaint of harassment should be made to your Supervisor, another management representative or the Human Resources Advisor. At the same time, a "Complaint of Harassment Form" (see "Harassment Personal Complaint Form"), with all of the appropriate details of the incident will be completed.

The Human Resources Advisor is Peggy Byrne Carter c/o Alexandra Marine and General Hospital (ext. 5720), email patricia.byrnecarter@amgh.ca.

Investigative Procedure

All complaints will be investigated promptly and confidentially by the Supervisor and/or the Human Resources Advisor. That person interviews the complainant, any witnesses, and the alleged harasser in an attempt to mediate a resolution between the parties. The complainant, the alleged harasser, the witnesses and any other persons involved in the investigation will hold all information in strict confidence and discuss the details only with those directly involved in the investigation. The interviewer, however, may discuss the matter with the CEO or another Supervisor or management representative for guidance or assistance after obtaining written consent from the complainant. The alleged offender and alleged victim have the right to be represented and accompanied by an individual of their choice during the interview related to the complaint. This process is to be completed with thirty (30) days.

If a physician is being harassed, a complaint of harassment should be made to the President of the Medical Staff. The President may discuss the matter with the Chief of Staff for guidance or assistance after obtaining consent from the complainant. After the investigation is completed, the complainant and alleged harasser will be advised of the outcome of the investigation within five (5) working days. The President/ CEO will be so advised. If the alleged harasser is the President/CEO, the Board Chair will be advised of the outcome of the investigation.

If it is determined that an allegation of harassment is valid, appropriate corrective action will be taken. The corrective action may include any one or more of the following:

- a formal written apology
- education sessions
- counselling through EAP (1-800-265-8310)
- verbal warning
- written warning
- suspension
- Credentials Committee
- discharge
- any reportable act committed by a professional will be reported to the their College
- The following criteria will be considered in determining appropriate correction action:
    - the nature of the harassment;
    - any record of previous offences, their nature and degree of severity;
    - disciplinary precedents for similar/previous offences; and
    - special or mitigating factors

The complainant and the harasser are informed about the result of the investigation, and any corrective action, in writing.

This program will be reviewed at least once a year.

Appeal Process

If an individual is unsatisfied with the outcome of the harassment investigation a complaint may be filed with the Ontario Human Rights Commission. Their website address is www.ohrc.on.ca. Their toll free number is: 1-800-387-9080. Their email address is: info@onrc.on.ca

Direct Enquiries To:

- Human Resources
- Your Supervisor
- Any Supervisor with whom you feel comfortable

Source: Ontario Human Rights Commission

Alexandra Marine & General Hospital	Freedom of Information & Privacy Manual	Initial Live Date: September-10-2012
Approved by: Corporate Leadership	Privacy - System Access - EPR Network and PACS Network	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

POLICY

Alexandra Marine and General Hospital is a partner in a regionally shared Electronic Patient Record (EPR) through the Thames Valley Hospital Planning Partnership (TVHPP) with the Huron Perth Healthcare Alliance (HPHA). The AMGH employees and affiliates, who provide Digital Imaging services for the organization, may be provided PACS Access privileges to this regionally shared PACS Network.

System Access including access to the electronic patient record EPR/Meditech, PACS, and related clinical applications at the AMGH will be granted to hospital employees and affiliates referencing their requirements as outlined in their job/position description/fact sheets. It is the responsibility of all AMGH employees and affiliates who have System Access and/or EPR/PACS Access to adhere to all privacy and confidentiality policies (as well as requirements outlined in the System Access Agreement form).

To ensure Systems Access including EPR/PACS Access, continues to be appropriate, audits will be conducted for compliance and inactivity.

Misuse, inappropriate access and/or disclosure of patient information from the EPR/PACS may be cause for disciplinary action up to and including suspension of systems access, termination of employment / contract, loss of privileges or affiliation with AMGH.

Procedure

Requesting Access

Human Resources will be responsible for requesting systems, EPR and/or PACS access for their existing and new employees or affiliate/end users. Human Resources will also ensure the following access requirements are met:

- complete a **Request for Network Resources Access** form for each new employee or affiliate/end user to their area, including service area transfers and forward to Information Systems;
- submit completed Request for Network Resources Access form to IS at least 7 business days before access is needed;
- specify a termination date for certain categories of hospital affiliates;
- complete a **System Access Agreement** form to report any changes to access requirements or employment status; and
- the Chief Executive Officer or Chief Information Officer must request access for Directors/Vice Presidents.

Occupational Health-Infection Control Coordinator will ensure the following requirements are met:

- completion of Privacy Education, including Privacy and Confidentiality Agreement policies review;
- Privacy and Confidentiality Agreement is completed and signed;
- all Systems Access and use policies are reviewed and agreements signed; and
- ensure the Privacy and Confidentiality Agreement and Systems Access Agreement forms are retained on the employee's personnel file.

Information Systems - Local Registration Authority ONLY will:

- be responsible for granting access to the organization's Systems Access, EPR and PACS;
- review and ensure completion of the Access Request form to grant appropriate systems access;

- retain Access Request form to support the granting of access to the EPR/PACS;
- track access in an Access Log as well as any modification, suspensions, terminations; and
- consult with Privacy Officer, and others as appropriate regarding new permission groups.

Employees, Affiliates and EPR/End Users must:

- comply with relevant corporate policies regarding privacy; confidentiality, information security, and all systems access including the terms set out in this policy and in the System Access Agreement form; and
- employees/affiliates will not be permitted to request their own access or changes to access. Certain categories of hospital affiliates and contract employees may be granted systems access on a time-limited basis and, unless extension is requested, access terminates automatically.

Requesting an Extension for Contract Staff/Affiliate Users Granted Temporary Access

The Manager or Delegate will:

- complete the 'Extend User Access' portion of the Access Request form to request an extension for access beyond their assigned termination date;
- forward the Extended User Access portion of the Access Request form to the Trusted User at least twelve business days before the assigned termination date; and
- follow the procedures when requesting NEW access if an extension is sought after the termination date.

Trusted User will:

- receive confirmation from the Manager; and
- forward the confirmation to the requesting Manager or Delegate.

Requesting the Disabling of Access
PACS Coordinator will coordinate all disabling of access based on changes in staffing.

Definitions

Local Registration Authority is a designated individual in the Information Systems Department who has special privileges and responsibilities regarding granting access to and managing EPR/PACS accounts and applications, security and other related administrative matters.

Directors are responsible for requesting access to EPR/PACS and notifying the Local Registration Authority about any significant changes in a user's duties, functions or role.

Employee refers to regular full-time/part-time or casual employees and contract employees who are paid directly by the organization.

Affiliates refers to individuals who are not employed directly by the organization but perform specific tasks at or for the organization, including appointed professional (e.g., physicians/midwives/.dentist), students, researchers, contractors, or contractor 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.

End User is an employee/affiliate who is granted access to the EPR/PACS to conduct hospital business activities.
Access Profile refers to individual's authorized abilities to perform certain actions and view certain kinds of patient information within the EPR/PACS. EPR/PACS access profiles are related to job/position descriptions.

Assigned Termination Date refers to the termination date assigned to EPR/PACS access accounts created for affiliates, excluding residents/fellows, and physicians. Accounts for selected affiliates terminate automatically on the assigned termination date unless an extension is requested.

EPR/Meditech refers to the electronic patient record that is generated for all patients through the hospitals operating system (computer software application) called Meditech.

PACS (Picture Archiving Communication System) refers to the Digital Imaging system.

References:

Corporate Policies

- LHSC Policy and personal correspondence, 2008
- Privacy Policy
- Confidentiality Agreement Policy
- Acceptable Use of Information Technology Resources Policy

Legislative Resources

- Personal Health Information Protection Act (PHIPA), 2004

Alexandra Marine & General Hospital	Freedom of Information & Privacy Manual	Initial Live Date: September-7-2012
Approved by: Corporate Leadership	Privacy - General Guidelines	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Policy

Basic Privacy Rules

Personal Health Information (PHI) is not to be left in written form or displayed on computer terminals in areas or locations where unauthorized individuals may access it, nor is to be stored on the "c:" drive of any hospital computer or portable storage devices or personal device assistants (PDAs). PHI is not to be left unattended where there is no one to receive the information (e.g. fax machines).

Random audits on the records of current and discharged patients are conducted on Alexandra Marine and General Hospital's information systems to ensure that users are only accessing PHI required for job purposes. Staff, Medical Staff, Volunteers, Students, Vendors, and/or any person/entity with access to records are included in random and/or focused audits.

Failure to abide by these guidelines may result in disciplinary action up to and including termination and/or discontinuation of privileges.

Strict adherence to the following rules is required:

1. DO NOT discuss PHI with the patient or any other interested party unless it is part of your role as a caregiver.

2. DO NOT discuss PHI regarding patients, patients' visitors, medical staff, or hospital staff:
   - in areas where the general public may overhear the discussion;
   - in public areas in the hospital such as corridors, elevators, cafeteria; (where the physical environment limits privacy options, extra care must be taken to respect the privacy rights and comfort levels of others);
   - at home; or
   - in public places outside the hospital.

3. DO NOT access patient PHI except in the course of performing your role as a healthcare provider for that patient.

4. DO NOT remove, copy or transmit PHI other than through those procedures outlined in the "Transmission of Personal Health Information by Facsimile" and "Release of Information" policies.

5. Apply the "Need to Know" rule:
   - If you do not need to know the information to perform your job function, do not look at it or collect it.
   - Do not "surf" for information on your friends, family or co-workers.
   - Ensure that the personal health information (PHI) you disclose is only the necessary information required by the other party.

6. Never share your computer password:
   - You are responsible for every entry done under your user id & password.
   - The person using your password may commit a breach of confidentiality.

7. If you are in doubt about the PHI you are going to release, seek express consent from the patient.

8. Never disclose PHI to anyone outside the "Circle of Care" without the express or implied consent of the patient, unless authorized by law (e.g. a police warrant). Implied consent means that a notice

about the disclosure is posted for the patient to see, and the patient has not refused or withdrawn consent.

9. When giving PHI over the phone to an authorized person, ensure that you verify the identity of the person (e.g. the call back principle).

10. Sign off your computer when stepping away from your workstation.

11. Be aware of those around you when sharing PHI.

12. Use a cover sheet when faxing confidential information and ask for a cover sheet when you are receiving one.

13. Never store PHI on a laptop, PDA or desktop. All PHI must be stored on the network.

14. Ensure appropriate measures are in place if sending Personal Health Information in an email.
    - Software to encrypt email is required (Consult IT)

15. Ensure PHI is disposed of properly and according to "Retention of Records Guidelines POLICY"
    - Dispose of any PHI that is not a part of the chart. (e.g. patient list) into designated shredder boxes, shredder machine, or a secure location.
    - Ensure that PHI on workstation is secure and out of view of the public.

16. Wear your ID badge at all times.

17. Verify legitimacy of unknown persons by checking their badges including picture

18. Reproduction or copying of any PHI should be limited and should not interfere with the integrity of the information. Agents reproducing or copying documents are responsible for ensuring that the documents are not left behind and that any discarded copies are shredded and disposed of securely.

Reference

Hospital Privacy Toolkit, OHA 2004

Alexandra Marine & General Hospital	MANUAL: Human Resources	Revision Date: February-5-2016
Approved by: Corporate Leadership	Respect in the Workplace Policy	Original Date: February-8-2013

POLICY OBJECTIVES:

- To promote an understanding of diversity;
- To foster courteous and respectful interactions;
- To ensure a workplace free from discrimination and harassment within the meaning of the Human Rights Code; and
- To resolve interpersonal issues at the earliest possible opportunity and with the least formality possible given the specific circumstances of the situation

POLICY STATEMENT AND INTENT:

Alexandra Marine and General Hospital (AMGH) is committed to providing a work and service environment that is characterized by respectful behavior and freedom from discrimination and harassment. AMGH recognizes the right of all people to be treated with dignity and respect, and believes that such an environment increases job satisfaction and, in turn, enhances teamwork, productivity and patients' experiences.

All persons associated with AMGH are responsible for their own conduct and as such must ensure their conduct is civil, respectful, cooperative and non-discriminatory in the workplace, in the community, and at work-related events. Persons include all employees, physicians, residents, Foundation staff, students, volunteers and contractors. AMGH will consider any incident resulting in disrespectful behavior or any incident resulting in discrimination very seriously and will take appropriate steps including imposing discipline where warranted, to ensure a respectful and cooperative workplace.

This policy does not limit the right of AMGH as an employer from exercising its management and supervisory rights appropriately and in good faith, including management of the performance of employees and managers. AMGH strongly supports education and conflict resolution as the means to achieve these goals and will provide staff with information, training and support in resolving respect in the workplace issues.

There is a zero tolerance for behavior that is in contravention to this policy.

DEFINITIONS:

I. Respect in the Workplace versus Disrespectful Behavior

Respectful workplace behavior incorporates courtesy, civility, consideration and compassion. It is an approach which actively respects individuals by avoiding behaviors which would be upsetting to them and engaging in basic polite behavior.

Examples of Courteous vs. Disrespectful Behavior

- Quiet and calm communication which focuses on the issues rather than personal characteristics

vs.

Loud, profane, name-calling, and abusive language that focuses on personal characteristics.

- Expressing disagreement in a calm and professional manner

vs.

Making threats, intimidation or insulting others.

- Addressing issues and concerns regarding performance or misconduct through the responsible managers

vs.

Engaging in malicious gossip, and rumors with intent to do harm.

- Sharing information required to deliver services effectively

vs.

Purposely ignoring questions or deliberately failing to provide necessary/helpful information.

- Legitimate supervisory responsibilities including constructive performance management

vs.

Being carried out in an abusive and derogatory manner.

II. Discrimination and / or Harassment

This Does NOT constitute Discrimination or Harassment:

- Following up on work absences or related attendance matters.
- Requiring and/ or managing performance to job standards
- Taking disciplinary measures
- Difference of opinion or a disagreement, or insubordinate behavior
- Acting in an abrupt manner relative to the seriousness or significance of a situation.
- Exclusion of individuals for a particular job based on specific occupational requirements necessary to accomplish the safe and efficient performance of the job

Discrimination

Discrimination is any comment or conduct which would constitute a breach of the Ontario Human Rights Code. It includes exposing a person to negative consequences, preferring a person, or changing a person's employment terms or conditions on the basis of: race, color, ancestry, place of origin, religion, marital status, family status, physical or mental disability, gender, sexual orientation, age, political belief, or if there is a criminal charge or conviction unrelated to the occupation of the person. It is important to note that such conduct is not only a breach of this policy but that it is also against the law.

Discriminatory Harassment

Discriminatory Harassment is a form of discrimination and is also contrary to the Ontario Human Rights Code. Discriminatory harassment is abusive, unfair, offensive or demeaning treatment of a person or group of persons related to the criteria in the discrimination definition that a reasonable person should have known to be unwelcome and unsolicited. It includes actions, comments, or displays.

It creates an intimidating, hostile or offensive environment for work or participation in work-related activities, and it may be a single incident or continuous over time. What generally constitutes harassment is serious or repeated rude, degrading or offensive remarks such as:

- Teasing about a person's physical characteristics or appearance or level of intelligence.
- Making disparaging comments or insults that are of a personal nature
- Targeting someone for meaningless or 'dirty jobs' that are not part of their normal duties.

Discriminatory Sexual Harassment

Discriminatory Sexual Harassment is a form of discrimination and is also contrary to the Ontario Human Rights Code. As such it is not only a breach of the policy but it also against the law.

Examples of Sexual Harassment:

• Requests for sexual favors, or other verbal or physical conduct of a sexual nature when submission to or rejection of such conduct becomes explicitly or implicitly a term or condition of employment or promotion.

• Unwelcome sexual remarks, invitations, or requests including persistent, unwanted contact after the end of an intimate relationship.

• Conduct or comments of a sexual nature that a reasonable person knows or ought to have known is unwanted and unwelcome or has the purpose or effect of interfering with work or performance.

• Comments or conduct of a sexual nature when such comments or conduct creates an intimidating, hostile or offensive working environment.

• Unwelcome or intimidating invitations or requests with sexual overtones, whether explicit or indirect.

• Actual reprisal or an expressed or implied threat of reprisal for refusal to comply with a request for sexual favors.

V. Complainant

The Complainant is any person or persons who seek recourse in relation to this Policy as someone who believes he or she has experienced lack of respect, discrimination or harassment as outlined in the definitions of what each constitutes.

VI. Respondent

The Respondent is any person or persons against whom an allegation of disrespectful behavior, discrimination or harassment has been made in relation to the Policy.

RESPONSIBILITIES UNDER THIS POLICY

AMGH Corporate Responsibilities:

- The Board of Directors enforces there is Policy and Process to govern respectful behavior within the organization.
- The CEO assumes overall accountability and responsibility for the Policy's effectiveness.
- Executive leaders are responsible for ensuring that the provisions of this policy are adhered to consistently within their portfolios.
- The Human Resources department is responsible for screening all formal complaints made under this Policy and may after consultation with the CEO refuse to proceed with a complaint under this policy if it does not meet the definition. It is responsible for facilitation and oversight of the complaint and investigation process in collaboration with the relevant executive leader and manager, and provides a report back to the CEO.

Managerial and Supervisory Responsibilities:

- Directors, managers and supervisors are expected to be role models to staff for appropriate workplace behavior. AMGH will assist and support directors, managers and supervisors in fostering a safe working environment free of harassment and in dealing with situations of harassment and disrespectful behavior when aware of them.

- Directors, managers and supervisors are responsible for respecting the confidentiality of anyone involved in a complaint, cooperating in the event of an investigation by both participating personally if called, and, enabling those in their workforce to participate.

Employee, Volunteer, Physician, Resident, Foundation Staff and Student Responsibilities:

- Each person has the responsibility to treat one another with respect, and the right and responsibility to speak to the appropriate person if they or someone else is being harassed or treated disrespectfully in the workplace.

- Each person is responsible for maintaining and respecting the confidentiality of all parties regarding any complaint under this Policy.

- Each person is responsible for participating cooperatively in an investigation and mediation whether informal or formal.

Unions and Professional Bodies

- AMGH recognizes that unions, medical and professional regulatory bodies are partners in maintaining a workplace free of harassment and discrimination and supportive of respectful workplace behavior. AMGH will work with these organizations to effectively implement and enforce the provisions of the Policy.

Alexandra Marine & General Hospital	Administration Manual	Initial Live Date: July-27-2012
Approved by: Corporate Leadership	Security	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Policy

Alexandra Marine and General Hospital endeavours to maintain a safe and secure environment, for our staff, patients and visitors and the prevention of theft from the facility and damage to property.

The security officer for AMGH is the Director, Support Services.

Security Training

- The security officer is responsible to ensure that staff, physicians, volunteers, and contractors are aware of this policy and adhere to its contents.
- The Occupational Health/Infection Prevention and Control Coordinator is responsible to ensure that new employees are oriented to hospital security policies.

Goals and Principles

Identification Badges

- All staff, volunteers, physician, students, and pastoral care team members, must wear their identification badge at all times while on hospital property.
- Staff are provided with an identification badge. There is a replacement charge to employees for lost cards.
- All outside service contractors, inspectors, and students or any other visitors that will be working in the hospital must wear a "Visitor Badge" or Company Badge. Visitor badges can be obtained at the Business Office.

Outside Workers

- If outside contractors/service technicians or inspectors will be in the facility "after hours", the department they are working in must notify the communication department and indicate how long they expect them to be in the building. These individuals will be instructed to report to the Switchboard Department when they depart to inform the department that they are leaving and to return any keys and/or ID badges.

Doors

- The Emergency Entrance is the 24-hour entrance to the building. The doors are open from 0530 to 2330. The doors must be locked from 2330 to 0530 by the staff at Switchboard. The Switchboard clerk provides access to the building when the doors are locked.
- The Door from the outpatient waiting room to the basement corridor is open from 0645 - 2030. The door is locked all other times. The Switchboard clerk is responsible for ensuring the door is shut at 2030 every evening.
- The Front Entrance to the hospital will be open from 0645 to 2030 Monday to Friday and from 1100 to 2030 on weekends and holidays. The Front Entrance doors will be locked at all other times.
- The North side entrance to the hospital is locked at all times. Staff are able to access the building through this entrance after these hours with their I.D. badge.
- The South entrance is locked at all times. Staff will be able to access the hospital with their I.D. badge.
- The entrance by stores will be opened and closed by the person working in stores. The entrance will be locked, if the person working in stores is out of the department.
- All departments must be locked at the end of shift and when no one is in the department.

- All doors to mechanical rooms and electrical rooms as well as the "tunnel" must be locked at all times.
- Exterior doors must not be "propped open".
- Switchboard staff will shut the door between the Emergency waiting room and the basement corridor at 2030.

Windows

- All windows must be closed when each department closes for the day.

Keys

- All keys and hospital ID badges are the property of AMGH and must be returned to the payroll / human resources department on termination of employment.
- Lost and damaged keys must be reported to the Director of Support Services.
- The employee is responsible for safeguarding the key during his/her term of employment.
- Spare keys are stored at Switchboard in a locked box. This box must be kept locked at all times. Keys must be signed in and out and a record must be kept of who signed out and returned keys. Only Switchboard staff may sign out keys. Non-Switchboard staff must ask Switchboard staff to sign out keys and not remove keys independent of Switchboard staff involvement.

Unattended Packages

- Any unattended bags, parcels and packages should be reported to the departmental supervisor or admin. on call. The supervisor or the admin. on call will advise if the OPP are to be notified. Isolate the area and do not touch the suspicious package

Visitors / Loitering

- Any visitors coming through the Emergency entrance after 2030 should be approached as to the reason for their visit by Communications. If there is not a valid reason they should be asked to leave.
- Visitors should not be allowed entry to the building after 2030 to use the bathroom, use the change machine, vending machines, etc.

Suspicious Behaviour

- The OPP should be called ANYTIME staff feel unsafe or threatened. Such instances include someone, who is loitering, someone who has no legitimate reason for being in the building or someone who is acting in an aggressive manner.
- If the OPP are contacted by the hospital, the administrator on call must also be notified.
- The Director or Administrator on call must be contacted of any theft or damage to property.

Staff

- Staff are encouraged to leave the building in pairs during evening and night shifts, if possible.
- Staff are required to follow any departmental specific policies related to security.

Cameras

- Cameras are not permitted within the hospital unless approved by Management or the Nurse in Charge of the Unit. Consent from the patient must be obtained before an image

All unexpected events must be entered in Risk Monitor Pro before the end of the shift.

Alexandra Marine & General Hospital	Information Technology Manual	Initial Live Date: September-30-2012
Approved by: Corporate Leadership	Social Media Policy	Review Frequency: Every 2 years

Any printed version of this document is only accurate on the date of printing. Always refer to the electronic version for the most current version.

Introduction

AMGH recognizes the importance of building strong relationships with our stakeholders and engaging community members in support of our operations.

Social media has become a popular form of communication used to build relationships both professionally and personally through electronic means. For professional uses, social media is vital in promoting meaningful dialogues and building relationships. It is also a useful tool for engaging both internal and external parties in the brand and services of the organization. AMGH recognizes the importance of professional interaction with stakeholder groups through social media platforms.

Due to the permanency, potential viral spread and real-time publishing abilities of social media platforms, a social media policy is necessary to govern interactions and manage legal, privacy and ethical issues related to social media use.

Policy

AMGH's social media accounts will be created and managed under the direction of the Chief Information Officer.

It is important for our organization to speak with one voice. In general, only one AMGH account should exist on a social media platform. This account will encapsulate the identity of all hospital departments and sites, while enforcing awareness of the hospital brand, direction and services. Programs or departments of the hospital must not set up social media accounts that are in any way affiliated with AMGH, without the prior consent of Chief Information Officer.

It is the responsibility of the Chief Information Officer to grant or terminate the necessary permissions required for the creation of social media accounts that represent AMGH; while also counseling, supervising and monitoring colleague use of social media as it pertains to the organization.

Any colleague who posts content to AMGH's social media accounts should do so in a manner that aligns with related organizational policies (i.e. Workplace Violence and Harassment Prevention Policy, Filming and Photography, Authority to Speak on Behalf of AMGH, Media Relations, Personal Health Information, Privacy Policy, etc.).

Employees participating in social media must follow these principles:

1. AMGH's commitment to maintaining the privacy of its patients and families is absolutely critical. To this end, staff:
    - Must adhere to the AMGH's Mission, Vision and Values in all comments and interactions.
    - Are prohibited from publishing any content that is specific to any patient, including patient's names and/or personal health information;
    - Are prohibited from providing medical details of a patient's case, even if the name of the patient is not disclosed.
    - Must not disclose the full names of other staff members, without their consent;
    - Must adhere to AMGH's privacy and confidentiality guidelines as they relate to patients, families, staff and all aspects of the business of AMGH.
    - Are prohibited from posting any patient or staff images or videos.

2. Comments which are discriminatory, such as those that refer to race, age, gender, sexual orientation, religion, political persuasion, physical or mental health and/or access issues, or any other factors identified in the Ontario Human Rights Code are prohibited.

3. Employees who have identified themselves on-line as AMGH employees (i.e. those who have listed their workplace in their profile) must not publicly support groups, petitions or causes that may be in conflict with AMGH's values and advocacy principles.

4. Employees must not post negative comments about AMGH, disclose sensitive internal information about AMGH or post any comments that could cause harm to AMGH's reputation or its employees, volunteers or physicians.

5. Employees must not post derogatory comments about other staff, or participate in any form of workplace gossip.

6. Social networking sites allow photographs, videos and comments to be shared with other users. It may not be appropriate to share work-related information in this way. For example, there may be an expectation that photographs taken at a private staff event will not appear publicly on the internet. Employees must be considerate to their colleagues in such circumstances and must not post photos without discussing it with them first and ensuring they are comfortable with it. If they later ask for the photo to be removed, it must be removed.

7. If employees maintain a web presence, i.e. blog, website, and such presence makes it clear that the author works for AMGH, it must include a simple and visible disclaimer such as "the views expressed on this blog are my own and do not reflect the view of my employer."

8. Employees must not agree to be "friends" and/or "like" on Facebook or other social media with patients, clients, and/or their families, while under their care, as this violates the therapeutic boundaries of the caregiver/patient relationship regardless of whether you try to "friend" them or they try to "friend" you.

9. Never post information or photos about patients, co-workers, or the confidential business information of the organization, even if you think it is unidentifiable.

Procedure

COLLEAGUE USE OF SOCIAL MEDIA:

Information posted on social media platforms is legally considered public material. This section will outline colleague interaction on social media through the use of personal social media accounts and in relation to stakeholder groups. All colleagues are responsible for clearly separating personal use of social media from their role at AMGH. Specifically:

1. Social media use by all colleagues is governed by the Confidentiality Policy and Workplace Violence and Harassment Prevention Policy.
   - The disclosure of proprietary or confidential information related to AMGH is strictly prohibited.
   - Communications on social media platforms should not humiliate, harass, bully or otherwise offend fellow colleagues; or damage the reputation of AMGH.
   - Individuals may be held liable for defamatory, proprietary or libelous commentary. Posting of such content may result in disciplinary action (up to and including termination), as outlined in the Code of Conduct Policy.

2. To maintain a professional relationship, colleagues must refrain from using their personal social media accounts to interact with patients on social media platforms. Colleagues must not encourage

or facilitate the release of personal health information or identifying information via social media platforms, and should not offer medical advice via social media posts.

3. A colleague who chooses to be active on social media platforms should take appropriate action to distinguish their personal opinions from those of AMGH. Colleagues who use social media to promote a particular product, service, or person, must clearly separate their opinions from those of the organization through a written statement resembling the following: "The views expressed on this social media account are solely mine and not those of my employer, AMGH."

4. AMGH reserves the right to block access to social media sites that do not promote a productive work environment. Excessive use of social media during shift hours is considered a performance issue and is assessed by management (at its sole discretion).

5. Colleagues using social media may be approached by a member of the media for comments concerning AMGH. All comments from media should be redirected to CEO Office as per the Media Relations Policy.

6. Social media posts by colleagues should not include the AMGH logo, identifying or defamatory images/videos of hospital grounds/property without the authorization of the Chief Information Officer.

7. The Chief Information Officer reserves the right to monitor all social media posts related to AMGH and its stakeholder groups.

USE OF SOCIAL MEDIA IN REPRESENTATION OF AMGH:
Approval to speak on behalf of AMGH via social media platforms will be designated through the Chief Information Officer. Specifically:

1. Representation of AMGH through the creation of a social media account or the ability to respond to social media posts related to AMGH is the sole responsibility of the Chief Information Officer.

2. Only one account per social media platform should represent AMGH. If required, the creation of additional social media accounts by colleagues may be considered following a needs assessment performed by the Chief Information Officer and approval from the CEO.

3. The purpose of an AMGH social media account should be aligned with the mission, vision, values and strategic directions of the organization and should not overlap a presence that already exists through other social media accounts.

4. All AMGH social media accounts must have a staff member who is designated as the "Administrator" of the account. Administrator responsibilities include:
    a. Creating the appropriate security settings for the account.
    b. Maintaining professionalism and appropriate boundaries throughout all interactions with stakeholder groups.
    c. Regularly monitoring and updating content on AMGH social media (NOTE: the definition of "regular" is dependent on the type of social media platform). If content on social media accounts is not monitored frequently, it is the responsibility of the Administrator to post, in a permanent location on the account, "Hours of Operation" for the account.
    d. Adhering to all related AMGH policies in their most current versions.
    e. Consulting with the Chief Information Officer to create a long-term social media strategy.
    f. Removing posts deemed inappropriate (i.e. spam or defamatory, proprietary or libelous commentary).

5. Social media accounts should promote and create a place for safe, open dialogue with stakeholder groups, All AMGH social media accounts should include the following components:
    a. The program description and image on the social media account must follow the current Corporate Standards Guides/Wayfinding Standards/Style Guide.
    b. In addition to including "Hours of Operation," AMGH social media accounts should display, in a permanent location, a note that social media accounts are not intended for medical information/diagnosis of medical concerns, or for medical emergencies. Administrators must speak to the Chief Information Officer regarding posts requiring immediate action (i.e. instances where a comment implies harm to an individual).
    c. Comments about AMGH should only be removed in extreme circumstances, and should be commented on or directed to the appropriate hospital department. Accounts should clearly outline when posts will be removed by an Administrator through a "Terms of Use" document.

6. Material (i.e. photos, videos, release of personal health information) posted by the Administrator pertaining to patients, colleagues or community members must be preceded by the signature of the appropriate consent form by the individual or their legal guardian.

Definition(s)

Social media

Is a two-way, Internet-based form of communication that facilitates interaction with individuals or entities through the sharing of real-time "posts" of electronic media content (i.e. photos, videos, articles/blogs, micro-blogs, forums wikis, websites, phrases [tweets, statuses], etc.). Social media "platforms" (also called social networking sites) can be specialized to a particular field of interest (i.e. professional networking), or can be targeted to the general population. Platforms include, but are not limited to: Foursquare, Facebook, YouTube, Twitter, Flickr, Pinterest, Blogger and LinkedIn.

Social media accounts

May be used to represent an organization in a professional manner, or may be used by an individual in their personal life. "Personal social media accounts" may be used by an AMGH colleague to interact with their family, friends or colleagues; a "AMGH Health social media account" is used to interact with stakeholder groups, on behalf of AMGH Health.

Stakeholder groups

In relation to social media are the various audiences AMGH wishes to reach through social media posts. They include, but are not limited to: community members; partners; potential donors for foundations; current and prospective volunteers; students and residents; current and prospective employees; government/municipal bodies; media outlets and reporters; physicians and patients.

Viral

Refers to the ability of social media content to spread through real-time sharing of social media content. The ability for information to go "viral" is impacted by each platform's "Terms of Use," which often outline how information posted on platform is royalty free, and can be shared or reposted without explicit permission from the poster.

References

Lakeridge Health. (2012, April 4). Social Media Policy and Procedures. Administration Manual.
Providence Care. (2011, May 30). DRAFT Social Media Policy. Administrative Manual.
Sunnybrook Health Sciences Centre. (2010, October 12). Social Media Policy and Guidelines for Use. Administration Manual, Corporate Policies
The Hospital for Sick Children. (2011, June 29). Use of Social Media Platforms for Work Related Purposes. Communications and Public Affairs.

Alexandra Marine & General Hospital	MANUAL: Human Resources	Revision Date: January-29-2016
Approved by: Corporate Leadership	Violence Prevention in the Workplace	Original Date: November-19-2012

POLICY

Mission

Alexandra Marine and General Hospital is committed to providing a safe, healthy and supportive working environment by treating our employees and clients with dignity, respect, care and compassion. Violence in the workplace can have devastating effects on the quality of life for our employees and on the productivity of the organization. The management of AMGH recognizes the potential for violence in the workplace and therefore will make every reasonable effort to identify all potential sources of violence to eliminate or minimize these risks through the Workplace Violence Prevention program. AMGH is committed to exhibiting a zero tolerance for violence, abusive and aggressive behavior. AMGH refuses to tolerate any type of workplace violence, within the workplace or at work-related activities. AMGH is committed to the expenditure of time, attention, authority and resources ensure a safe and healthy working environment for all employees and clients for whom we provide care.

Purpose

AMGH has a "zero tolerance" approach to workplace violence. "Zero Tolerance" means that every reported action of abusive/aggressive or threatening behavior will be tracked and resolved based on the individual facts. Individual cases may require different resolutions. Although measures will be put in place to assist parties in conflict resolution, disciplinary action will be taken, where appropriate up to and including termination of employment, revocation of physician's privileges or termination of volunteer/student/contract agreements.

The purpose of the policy is:

- To promote a work environment whereby every individual feels free from any kind of threatening behavior;
- To link and add credence to our Standards for Behaviours of Excellence and enhance the standard of respectful behavior to all members of AMGH;
- To create practical links to already existing policies and procedures (Standards for Behaviours of Excellence, Health and Safety Policy, Harassment Policy, Patient Rights and Responsibilities and Code White);
- To provide staff, physicians, volunteers, students and contract employees with effective tools and strategies to be used within AMGH to prevent and respond to incidents of abuse and aggression in the workplace;
- To make available information regarding ways to identify those who potentially may be abusive or aggressive, especially with regard to the signals that may predict an incident of abusive and aggressive behavior and therefore prevent these from occurring;
- Raise awareness at AMGH regarding prevention of abusive and aggressive behavior at work;
- Establish a comprehensive reporting and tracking mechanism to document and investigate incidents that threaten the safety of our staff and wellness of our environment;
- Educate patients/visitors to AMGH about our "Zero Tolerance" for violence in the workplace;
- Provide the necessary physical and emotional support to those who perceive they have been victims of aggression/violence at work.

This policy was developed by the Environmental Team. The Joint Health and Safety Committee, Senior Management and Human Resources were consulted throughout the development of policy and program.

The following legislations were consulted in establishing this policy:

- The Occupational Health and Safety Act

- The Criminal Code of Canada
- The Ontario Human Rights Code
- The Workplace Safety and Insurance Act, 1997
- The Compensation for Victims of Crime Act
- The Regulated Health Professions Act

Definitions

AMGH is committed to providing a working environment free of violence by ensuring that all workplace parties are familiar with the definitions of workplace violence and their individual responsibilities for prevention and corrective action. For the purpose of this policy, "violence" is any actual, attempted or threatened behavior of a person that causes or is likely to cause physical and/or psychological harm/injury/illness or that gives a person reason to believe that s/he or another person is at risk of physical or psychological harm/injury/illness, including, but not limited to, any actual or attempted assault (includes sexual assault and physical attacks); threat; verbal, psychological or sexual abuse; and harassment. (From the Ontario Safety Association for Community & Healthcare)

Classifications of Violence in the Workplace

Type I	(Criminal Intent) committed by a perpetrator who has no relationship to the workplace
Type II	(Client) the perpetrator is a client at the workplace who becomes violent toward a worker or another client
Type III	(Worker to Worker) the perpetrator is an employee or past employee of the workplace
Type IV	(Domestic Violence) Also known as domestic abuse, spousal or child abuse. The perpetrator has an intimate relationship with an employee

Definitions Associated with Workplace Violence

Assault: any intent to inflict injury on another, coupled with an apparent ability to do so; any intentional display of force that causes the victim to fear immediate bodily harm. E.g. slapping, shoving and pushing, punching, kicking.

Harassment: engaging in any vexatious comment or conduct that is known or ought reasonably to be known to be unwelcome, and causes the person to believe their health and safety are at risk.

Near Miss: an act of striking out, but missing the target.

Physical Attack: an act of aggression resulting in a physical assault or abuse with or without the use of a weapon. Examples include hitting, shoving, pushing, punching, biting, spitting, groping, pinching or kicking the victim, unwelcome displays of affection or inciting a dog attack.

Property Damage: intentional damage to employees' personal property or to the AMGH property (throwing of any object, vandalism to employee's car, kicking or hitting fixtures and fittings, banging or throwing equipment).

Psychological Attack: an act that provokes fear or diminishes an individual's dignity or self-worth or that intentionally inflicts psychological trauma on another.

Sexual Abuse: any unwelcome verbal or physical advance or sexually explicit statement, displays of pornographic material, pinching, brushing against, touching, patting or leering that causes the person to believe their health and safety is at risk.

Sexual Assault: the use of threat or violence to force one individual to touch, kiss, fondle or have sexual intercourse with another.

Threat: a communicated intent (verbal or written) to inflict physical or other harm on any person or to property by some unlawful act. A direct threat is a clear and explicit communication distinctly indicating that the potential offender intends to do harm, for example, "I am going to make you pay for what you did to me." A conditional threat involves a condition, for example, "If you don't leave me alone you will regret it." Veiled threat usually involves body language or behaviors that leave little doubt in the mind of the victim that the perpetrator intends to harm.

Verbal Abuse: the use of vexatious comments that are known, or that ought to be known, to be unwelcome, embarrassing, offensive, threatening or degrading to another person (including swearing, insults or condescending language) which causes the person to believe their health and safety are at risk.
Workplace: Any location where any employee of AMGH is carrying out any work related function.
Examples

- All hospital buildings and property located on Napier and Montcalm Street, includes parking, old "ambulance base" and 108 Montcalm
- All Community Psychiatric Facilities – Goderich, Exeter, Wingham, Seaforth and Clinton
- Employee accompanied patient transport
- Any location where an employee is required to visit a client in the home
- Any location an employee is required to be during the course of their employment duties

Definitions of Employees
Contract Employees: Contract Employees includes any person paid for work by AMGH or working for a company hired to perform contract work at AMGH
Physicians: Any physician granted privileges of any kind with AMGH. Although not strictly defined as "employees" of AMGH, physicians will also be held accountable to this policy in course of their activities within AMGH. This group also includes residents and other physician groups in training
Staff: Staff includes all employees, permanent, temporary, and casual. Employees may be located in any department or site of AMGH and may be serving the organization in any capacity.
Students: Students include any university and other students who spend part of their academic course time within the AMGH community.
Volunteers: Volunteers include all those who give their time freely to the organization in service to the patients and staff of AMGH; and include members of the Hospital Foundation and Board of Supervisors.

Roles and Responsibilities of Workplace Parties
CEO and Executive Leadership Team
The CEO, together with the Executive Leadership Team, has the responsibility for health and safety and well-being of staff. Therefore, it is the responsibility of this group to implement the following:

- Model the substance and intent of the AMGH policy and Procedure for Workplace Violence and Prevention, and demonstrate in their words and actions as leaders of AMGH, commitment to intolerance of abuse and aggression of any kind within the organization.
- Accept responsibility for the provision of resources to train those in positions of leadership and to attend training themselves.
- Sign a Statement of Commitment to the Prevention of Violence in the Workplace annually.
- In consultation with The JHSC and The Environmental Committee, conduct regular risk assessments, control measures, and training and education. i.e. mandatory Code White training for all hospital employees.
- Ensure appropriate mechanisms / systems are in place to determine safe staffing levels for high-risk environments.
- Review all reports of violence or threats of violence in a prompt, objective and sensitive manner. This includes a review of all investigations associated with violence-related incidents.
- Take corrective action.
- Provide response measures.
- Facilitate medical attention and support for all those either directly or indirectly involved.
- Ensure any deaths or critical injuries have been reported to a Ministry of labor (MOL) inspector, the police (as required), the JHSC and union and investigated with the JHSC, and that a report goes to all parties in writing within 48 hours of the occurrence on the circumstances of the occurrence, including such information and particulars as the Occupational Health and Safety Act and regulations prescribe.

- Ensure a report goes to WSIB of all accidents where a worker loses time from work, requires health care, earns less than regular pay for regular work, requires modified work at less than regular pay or performs modified work at regular pay for more than seven days. Copies of accident information (where there is no critical injury) must be provided to the JHSC and union within four days of the occurrence, as the Occupational Health and Safety Act and Regulations prescribe.

Supervisors (including Departmental Managers)
Those who are in positions of responsibility for the health and safety and well-being of staff of AMGH must demonstrate in their attitudes and behavior the highest regard for the respect and dignity of all under their charge. Therefore all Supervisors must:

- Model the substance and intent of the AMGH Workplace Violence Prevention Policy and Procedure, and demonstrate in their words and actions as leaders of AMGH commitment to intolerance of abuse and aggression of any kind within the organization.
- Attend appropriate training regarding Workplace Violence.
- Sign a Statement of Commitment to the Prevention of Violence in the Workplace annually.
- Educate and train all direct staff in safe working practices regarding the creation of respectful work environments.
- Identify and alert staff to violent patients and hazardous situations.
- Ensure staff participation in educational and training programs to be able to respond appropriately to any incidence of work place violence. i.e., mandatory Code White training.
- Investigate all workplace violence using the Risk Incident Reporting System (RL6) procedure and form, and contact the police department as required.
- Facilitate medical attention for employee(s) as required.
- Ensure that debriefing is completed for those either directly or indirectly involved in the incident.
- Contact human resources to ensure the employees receive further counseling about the employee's legal rights.
- Track and analyze incidents for trending and prevention initiatives.
- Immediately report a death or critical injury to a Ministry of Labor (MOL) inspector. The police (as required), JHSC and union, and investigate with JHSC and report to all parties in writing within 48 hours of the occurrence the circumstances of the occurrence, including such information and particulars as the regulations prescribe.
- Issue a report to the employer and WSIB on all accidents involving lost time, where a worker requires health care, earns less than regular pay for work, requires modified work at less than regular pay or performs modified work at regular pay for more than seven days. Copies of accident information (where there is no critical injury) must be provided to the JHSC and union within four days of the occurrence, as the Occupational Health and Safety Act and regulations prescribe.

Employees and Physicians
Every individual employee/physician contributes to the creation of a safe and healthy work environment by demonstrating respectful and appropriate conduct at work.
All employees/physicians must accept as a personal responsibility their own role in eliminating the use of abuse and aggression in the day-to-day activities of their own work unit. Therefore employee's and physicians must:

- Participate in education and training programs to be able to respond appropriately to any incident of workplace violence. i.e. mandatory Code White training.
- Understand and comply with the violence in the workplace prevention policy and all related procedures.
- Report all incidents or injuries of violence or threats of violence to their Supervisor (designate) or CEO immediately, completing the Risk Incident Reporting System (RL6) report form.
- Contribute to risk assessments.
- Seek support when confronted with violence or threats of violence.

- Seek medical attention.
- Uphold the Standards for Behaviours of Excellence and its Principles.
- Sign a Statement of Commitment to the Prevention of Violence in the Workplace yearly.
- Reduce workplace violence by challenging workplace violence.
- Promote respectful interactions at work.

This is also expected from the employee/physician who witnesses an incident and is not the direct victim. Silence in the face of abusive behavior does not allow for promotion of a safer environment and so every employee/physician who witnesses abusive behavior is expected to report such behavior. No employee/physician who in good faith registers a complaint of abuse or reports an incident of aggressive behavior will suffer any recrimination for doing so. However, false and malicious accusations of abusive or aggressive behavior will face consequential corrective and remedial action with disciplinary actions up to and including termination.

All complaints and reports of abusive or aggressive behavior will be treated seriously, will be investigated thoroughly and fairly, and will be dealt with accordingly.

Patients, Family Members, Volunteers, Students, and other Visitors

Patients, family members, volunteers, students, and other visitors to AMGH can expect to be treated with dignity and respect at all times. They should not be expected to find abusive or aggressive environment when they come to use the services or are visiting AMGH for any reason.

It is also the expectation that patients, family members, volunteers and visitors will treat AMGH staff with the same respect and dignity, and that they do not exercise abusive or aggressive behavior towards members of the AMGH staff.

AMGH is committed to the following:

- Developing written communication for patients, family members and visitors outlining acceptable conduct that is expected for all people within the confines of AMGH.
- Signage throughout AMGH that sets out explicitly that AMGH has a Zero Tolerance for Violence, Abusive and Aggressive Behavior.
- Ensuring that all patients, family members and visitors are made aware of their rights and to seek recourse for perceived breaches of this Policy.
- Ensuring that all patients, family members and visitors are made aware of the consequences for them for breaches of the Policy.

Joint Occupation Health and Safety Committee (JHSC)

- Be consulted about the development, establishment and implementation of violence measures and procedures (the violence prevention program).
- Be consulted and make recommendations to the employer to develop, establish and provide training in violence measures and procedures.
- Take part in a review at least annually of the workplace violence prevention program.
- The worker designate should investigate all critical injuries related to violence.
- Receive and review reports of any critical injury or death immediately and in writing outlining the circumstances and particulars as prescribed within 48 hours of the occurrence.
- Review written notice within four days on lesser injuries where any person is disabled from performing his or her usual work or requires medical attention.

Reporting and Investigation

- Employees/ Physicians are to report all violence-related incidents or hazards to their Supervisor (designate).
- The Supervisor (designate) receiving the report investigates the report and ensures that measures are taken to safeguard employees and curtail the violence.
- The employer reports all injuries to the MOL and WSIB as required by the Occupational Health and Safety Act and Workplace Safety and Insurance Act.

- Team debriefing

Risk Assessment
Senior Management (with worker involvement) assesses workplace violence hazards in all jobs, and in the workplace as a whole. Risk assessments are reviewed annually and whenever new jobs are created or job descriptions are substantially changed.

Education
All new employees will receive both general and site-specific orientation to the Workplace Violence Prevention Program. In addition, all employees will receive an annual review of both the general and site-specific components of the program.
Any training developed, established and provided shall be done in consultation with and in consideration of the recommendations of the Joint Health and Safety Committee.

Program Evaluation
The effectiveness of the Workplace Prevention Program is evaluated annually by Senior Management and reviewed by the Environment Team and Joint Health and Safety Committee.
Workers and Supervisors (designates) are accountable for the policy and procedures related to workplace violence. This is part of the responsibilities to comply with health and safety policy workers job description. CEO and Supervisors (designates) responsibilities for enforcing policy and procedures, investigation of and response to workplace violence are also included in health and safety components of job descriptions.

Records
All records of reports and investigations of workplace violence are kept for five years.

Policy Review
This policy will be reviewed annually or more frequently if necessary, upon advice of the JHSC, the employer, or if there are any changes in circumstance that may affect the health and safety of a worker.

Approval Process	• Joint Health and Safety Committee – January 29, 2016 • Senior Administration Team – January 29, 2016