|  |  |  |
| --- | --- | --- |
| Technology Usage Policy**(E-mail, Computers, Internet, Phones, Facsimile, Scanning, Copiers, and Data Transmission)** | **Last Revision:** | November 2015 |
| **Last Reviewed:**  | November 2015 |
| **Applies to the following THA Group of Companies:** | * Island Health Care
* Island Hospice
* Independent Life at Home
* Ideal Aging
* RightHealth®
* THA Services
 |
| **Included in the following THA Manual:** | Administrative Policy & Procedure ManualManagement of Information |

**PURPOSE**

This policy broadly covers all of the THA Group’s technology resources – hardware, software, and content; this includes but is not limited to electronic networks, systems, computers, devices, telephones, software, data, files, and all content residing in any of these - referred to as “IT resources”. This policy applies to all records of THA Group and to the information in those records, regardless of the form or the location.

The purpose is to provide guidance for the appropriate use of electronic mail, Internet, mobile phones, facsimile, scanning devices, copiers, and data transmissions at THA Group, Inc. and to ensure the privacy and confidentiality of patient and corporate data within the organization.

**SCOPE**

This policy applies to all Employees, Volunteers, and Independent Contractors of THA Group. Unless expressly authorized by the Chief Information and Administrative Systems Officer, downloading, sending, transmitting, or otherwise disseminating proprietary information, trade secrets, or other sensitive privacy act information is strictly prohibited. Furthermore, no personally identifiable health information should be sent by public or private electronic networks without adequate safeguards against interception and/or misuse. A copy of this policy will be given to all employees at orientation.

The following sections outline the specifics of this Policy and Procedure for each area:

* + 1. **COMPUTERS**
		2. **INTERNET**
		3. **E- MAIL**
		4. **FACSIMILIE/SCANNERS**
		5. **MOBILE PHONES**

1. **COMPUTERS**

#### Authentication Process:

The employee-user must first be authenticated through a THA Group assigned username and password. The username and password is the responsibility of the individual to whom it is assigned. Any authorized use of the username and password by other individuals to gain access to the THA Group network and Internet makes that employer-user responsible for any and all actions of those individuals. Violations of THA Group Technology Usage Policy and any other policy through the authorized use of the username and password subjects the individual to whom it is assigned to disciplinary action, up to and including termination. One should not expect that transmissions made through the THA Group network are confidential. Although users are given a username and password, this does not insulate transmissions from employer review for business purposes.

**Licensed Software:**

Employee-users should take care to use THA Group software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

**Company issued Laptops:**

Employees who are issued company laptops must abide by the terms within this policy plus agree to the terms listed in the “Laptop Agreement” contract found at the end of this policy.

**Archiving Files:**

Employees should routinely clean off files from the computer to efficiently use the server – deleting unnecessary and temp files and archiving files on an annual basis.

#### INTERNET

**Internet Usage**:

Access to the Internet through THA Group network is a privilege and carries responsibilities reflecting responsible and ethical use. Use of the Internet through THA Group network constitutes the individual’s acceptance of this policy.

Employee-users are expected to be knowledgeable of these and all policies of THA Group. Care must be taken by all employee-users to ensure that accessing the Internet does not jeopardize THA Group interests. Any questions should be directed to the Chief Information and Administrative Systems Officer. Violations of this and any other THA Group policy subjects the employee-user to immediate revocation of system privileges and may result in further disciplinary action, up to and including termination.

#### Personal Use of Internet:

Limited personal use of the Internet is allowed by THA Group. However, the employee-user is reminded that use of any and all THA Group property is primarily for the purpose of THA Group business. Any personal use of the Internet is expected to be on the user’s own time and is not to interfere with the person’s job responsibilities. In addition, any postings to public forums such as newsgroups, or any transmittal of electronic mail through the Internet for personal use must include a disclaimer that the views of those the employer-user and not the THA Group. These forums should be used with care and not cause any adverse publicity or embarrassment to THA Group.

#### Ethical Use of Internet:

At any time and without prior notice THA Group management reserve the right to examine email, personal file directories, and other information stored on THA Group computers. This examination helps to ensure compliance with internal policies, supports the performance of internal investigations, and assists the management of information systems. As such, the Chief Information and Administrative Systems Officer may monitor access to the Internet. Use of the Internet constitutes acceptance of such monitoring.

This policy should be read and interpreted in conjunction with all other THA Group policies including but not limited to policies prohibiting harassment, discrimination, offensive conduct or inappropriate behavior. Employee-user are prohibited from accessing the Internet for any unethical purposes, including pornography, violence, gambling, racism, harassment, or any illegal activity. Employee-users are forbidden from using profanity or vulgarity when posting electronic mail via the Internet or posting to public forums (i.e., newsgroups). Any electronic mail sent through or postings to public newsgroups must fall within these ethical standards.

The employee-user must abide by all federal and state laws with regard to information sent through the Internet. THA Group Code of Ethics strictly prohibits unauthorized release or disclosure of any information through the Internet or any other means. Company trade secrets and confidential information should not be transmitted over the Internet.

Employee-users are also prohibited from using Internet access through THA Group systems for any other business or profit-making activities.

In general, employees should exercise the same restraint and caution in drafting and transmitting messages over the Internet as they would when writing a memorandum and should assume that their message will be saved and reviewed by someone other than the intended recipients.

#### Downloading Software:

Employee-users are prohibited from downloading software from the Internet without prior written approval of the Chief Information and Administrative Systems Officer or designee. Downloading of games from the Internet is prohibited. Downloading of any executable files or programs, which change the configuration of the system by anyone other than Information Services personnel, is prohibited. The employee-user should take extreme caution when downloading software or files from the Internet. All files or software should be passed through virus protection programs prior to use. Failure to detect viruses could result in corruption or damage to files and/or unauthorized entry into THA Group’s network. It is mandatory that you comply with copyright and trademark laws when downloading material from the Internet.

If the employee-user finds that any damage occurred as a result of downloading software or files, the incident should be reported immediately the Network Administrator or Chief Information and Administrative Systems Officer.

Employee-users may not install other on-line services to access the Internet on THA Group-owned computers, such as America On Line, CompuServe, Earthlink, Bellsouth, etc. Any questions should be directed to the Network Administrator or Chief Information and Administrative Systems Officer.

1. **E-MAIL**

**Official Means of Communicating:**

There is an expanding reliance on electronic communication at THA Group. Because of this increasing reliance and acceptance of electronic communication, e-mail is considered an official means for communication within the company. Implementation of this policy ensures that employees have access to this critical form of communication.

This company e-mail policy provides guidelines regarding the following aspects of e-mail as an official means of communication:

* Company use of e-mail
* Assignment of employee e-mail addresses
* Employee use of and responsibilities associated with assigned e-mail addresses;
* Expectations of e-mail communication

**Email Usage:**
E-mail is an official means for communication within the THA Group community. Therefore, employees have the right to send communications via e-mail and the right to expect that those communications will be received and read in a timely fashion.

**Assignment of E-mail Addresses:**
The Chief of Information and Administrative Systems Officer will assign all employees an official THA Group e-mail address. It is to this official address that the company will send e-mail communications; this official address will be the address listed in the company Global address book and on the employee section of the website. THA Group owns the electronic mail service, and considers electronic-mail private, direct communication between sender and recipient(s) or recipient(s)' designee(s); however, employees cannot expect absolute confidentiality. The contents are not monitored, observed, viewed, displayed or reproduced in any form by anyone other than the sender and recipient(s) or recipient(s)' designee(s) unless specifically authorized by the Privacy Official, a law enforcement representative or the Information Security Official.

**Expectations Regarding Employee Use of E-mail:**
Employees are expected to check their official e-mail address on a frequent and consistent basis in order to stay current with company communications. THA Group requires checking e-mail **twice daily** at minimum, in recognition that certain communications may be time-critical. In the event of a time-critical communication, a text alert will be sent instructing employees to read email for further information.

**Retention and Deletion of e-mails:**

Electronic mail is maintained in computer systems and on backup media for varying lengths of time and may be recovered subsequent to deletion. The messages may be disclosed in the same manner as paper records. Reasons for recovery of electronic mail messages may include legal discovery, external investigations by law enforcement personnel and internal security investigations.

**Redirecting of e-mail to a Personal address:**
An employee may have e-mail electronically redirected to another e-mail address. If an employee wishes to have e-mail redirected from his or her official address to another e-mail address (e.g., @aol.com, @hotmail.com), they may do so, but at his or her own risk. THA Group will not be responsible for the handling of e-mail by outside vendors. Having e-mail redirected does not absolve an employee from the responsibilities associated with communication sent to his or her official e-mail address.

**Appropriate use of employee e-mail:**

* 1. In general, e-mail is not appropriate for transmitting sensitive or confidential information unless its use for such purposes is matched by an appropriate level of security (i.e. communications involving patient records are HIPAA compliant). Never forward patient-identifiable data to a third party without the patient's express permission. Emails with sensitive information should be encrypted.
	2. Company e-mail is for business-use only and is not to be used to solicit for personal benefit.
	3. Slanderous or defamatory language is strictly prohibited. Material that is sexually explicit, obscene, embarrassing, fraudulent, hostile, harassing, or otherwise inappropriate or unlawful may not be forwarded or sent by electronic communication or displayed on or stored on company computer resources. Users receiving or viewing this kind of information must immediately report the incident to the Chief Information and Administrative Systems Officer.
	4. Every outgoing email address should be verified before sending. All outgoing emails automatically have the following confidentiality statement included at the bottom of emails:

	**CONFIDENTIALITY STATEMENT:**This message contains information which is privileged and confidential and is solely for the use of the intended recipient. If you are not the intended recipient, be aware that any review, disclosure, copying, distribution or use of the contents of this message and any attachments is strictly prohibited. If you have received this message in error, please destroy it and immediately notify THA Group, Inc. at 912-629-2727.
1. **FACSIMILIE / SCANNERS / COPIERS**

All staff must take precautions when using facsimile (fax), scanners, or copying machines to transmit documents.

Facsimile, Scanning, or Coping machines are not located in areas accessible to the general public, unless the equipment is intended for public use. In this case the publicly available equipment may not be used by staff members to send or receive faxes/scans containing patient information of any kind.

Staff shall not use company facsimile/scanning machines for transmitting personal documents. Facsimile/Scanning machine cover pages include the following information:

1. The sender's name, business address, business phone number, and business facsimile machine number;
2. the recipient's name, business address, business phone number, and business facsimile machine number;
3. transmission time and date (if not stamped by facsimile machine or computer);
4. classification of the document (CONFIDENTIAL documents).

Staff should verify the facsimile machine number of the recipient before transmitting.

A recipient of a document containing CONFIDENTIAL information (e.g., for the recipient's eyes only or containing patient-identifiable information) must be notified by phone before the document is transmitted. If at all possible, this type of document should not be faxed.

All pages, including the cover page, of CONFIDENTIAL documents to be faxed must be marked "Confidential" before they are transmitted.

Time, date, sender, recipient, and sender or recipient phone number for all materials sent and received by facsimile machine should be documented in a facsimile machine log to be kept with the facsimile machine. It is crucial that no personal health data be explicitly revealed in this log.

1. **MOBILE PHONES**

#### Personal Phones:

While at work employees are expected to exercise the same discretion in using personal mobile phones as is expected for the use of company phones. Excessive personal calls during the workday, regardless of the phone used, can interfere with company productivity and be distracting to others. A reasonable standard is to limit personal calls. Employees are asked to make personal calls on non-work time to ensure that friends and family members are aware of the company’s policy. Flexibility will be provided in circumstances demanding immediate attention.

The company will not be liable for the loss of personal phones brought into the workplace. Mobile phones should be turned off or set to silent or vibrate mode during meetings, conferences and in other locations where incoming calls may disrupt normal workflow.

#### Camera Phones:

.

Only photographs for assessment/diagnostic purposes (ex., wound care consults) are allowed. No identifying information shall be included in or with the photograph to protect patient privacy. The recipient of the photo is made aware of it’s being sent immediately before or after transmission.

#### Personal Use of Company-Provided Mobile Phones:

Where jobs or business needs demand immediate access to an employee, the company may issue a business-owned mobile phone to an employee for work-related communications. Employees who are issued company mobile phones must abide by the terms within this policy plus agree to the terms listed in the “Mobile Phone Agreement” contract found at the end of this policy.

 To protect the employee from incurring a tax liability for the personal use of this equipment, such phones are to be used for business reasons only. Phone logs will be audited regularly to ensure no unauthorized use has occurred.

Employees in possession of company equipment such as mobile phones are expected to protect the equipment from loss, damage, or theft. Upon resignation or termination of employment, or at any time upon request, the employee may be asked to produce the phone for return or inspection. Employees unable to present the phone within the time frame requested may be expected to bear the cost of a replacement.

Employees who separate from THA Group with outstanding debts for equipment loss or unauthorized charges will be considered to have left employment on unsatisfactory terms and may be subject to legal action for recovery of loss.

**Text Messaging on Company Phones:**

Employees in certain job classifications may be permitted to use text messaging as a communications tool. Texting on company phones is to be used only in the context of fulfilling one’s job duties and should not be used for personal communications. Text messages must adhere to all applicable privacy laws and regulations; specifically, messages should never contain protected health information or other information that is considered confidential.

Employees who use text messaging on company phones in the course of their work day should be mindful of the fact that texting while driving is prohibited by law. Employees who are issued citations for such acts will be liable for any fines imposed and will be subject to discipline under the company’s Performance Corrective Action policy.

#### Safety Issues of Mobile Phone Use:

Employees whose job responsibilities include regular or occasional driving and who are issued a mobile phone for business use are expected to refrain from using the phone while driving unless using a hands free system. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call. If acceptance of a call is unavoidable and pulling over is not an option, employees are expected to keep the call short, use hands free options if available, refrain from discussion of complicated or emotional discussions and keep their eyes on the road. Special care should be taken in situations where there is traffic, inclement weather or the employee is driving in an unfamiliar area.

Employees whose job responsibilities do not specifically include driving as an essential function, but who are issued a cell phone for business use, are also expected to abide by the provisions above.

Employees who are charged with traffic violations resulting from the use of their phone while driving will be solely responsible for all liabilities that result from such actions.

#### Courtesy Issues

As a courtesy to others and out of respect for fellow team members, company and personal phones should be turned off or set to silent/muted or vibrate/manner mode during meetings, conferences and in other locations where incoming calls may disrupt normal workflow.

**PROCEDURE**

Performance Excellence will review this policy as needed. Changes will be authorized by the approval of the Coordinating Council. Employees with questions or comments about this policy should contact the Chief Information and Administrative Systems Officer.

Refer to the Acceptable Technology Usage Agreement, Laptop Agreement, Mobile Phone Agreement located at [\\Tha-fs1\2006\Approved Forms 2015\Technology Usage Forms](file:///%5C%5CTha-fs1%5C2006%5CApproved%20Forms%202015%5CTechnology%20Usage%20Forms).