



New Hope Services, Inc.

New Hope Development Services, Inc.

## IT Policy Manual

Revised September 2023

A handwritten signature in black ink that reads "Jody Heazlitt". The signature is written in a cursive style with a horizontal line underneath it.

Jody Heazlitt, President

TABLE OF CONTENTS

**OVERVIEW.....3**

**INTERNET USAGE ..... 3**

**EMAIL USAGE ..... 4**

**CELL PHONE USAGE..... 5**

**HARDWARE/SOFTWARE USAGE..... 6**

**HARDWARE ACQUISITION/DISPOSAL/TRACKING ..... 7**

**DATA PROTECTION.....8**

**EMERGENCY ASSISTANCE.....10**

# OVERVIEW

## INTRODUCTION

The Companies' (New Hope Services, Inc. & New Hope Development Services, Inc.) mission is to provide services responsive to individual needs. With the ability to work remotely, and the greater inclusion of software in day-to-day work, technology is key to providing and documenting those services in a more efficient manner. The IT Policy Manual describes the many uses of technology within the organization, and provides rules for staff members utilizing hardware and software.

## ORIENTATION

When a staff member is hired, their orientation includes a section covering technology. Conducted by the IT Department and others as needed, this IT orientation is an overview of the role of technology related to their position. Staff will be instructed how to access and navigate relevant software including, but not limited to: signing onto the network, email/webmail, Office 365 apps, TimeWorks Plus, and the New Hope portal.

## INTERNET USAGE

The Internet is a central component in how The Companies conduct business. Staff are connected through many functions of the Internet, and the leadership wants staff to be able to effectively use this resource in a productive and secure way.

## INTERNET USE AND SECURITY

When accessing the Internet through our servers or via Wi-Fi, it is important to remember the following points:

- Staff members are granted access to the network based on job description and duties. Some staff will have remote access while others will not. Remote access is only granted to those that require access to perform essential job duties.
- When accessing the Wi-Fi, please be sure to enter the password. This will be provided during orientation, or through an IT request on the portal (see software section for further information on the portal).
- Staff should never click on unfamiliar emails, attachments, links, or pop-ups. They may contain a virus, malware or be of other malicious nature and could infect your computer or our entire system. If you are unsure about an email, link, or pop up, **DO NOT CLICK**. At a minimum, you should report the email using Phish ER or contact the IT department prior to proceeding.
- Personal Internet use is **not** allowed.
- The Companies seek to create a productive and positive work environment. To help achieve that, staff should not view, download, create or distribute any inappropriate content or material.
  - Inappropriate content includes, but is not limited to: pornography, material that creates an unsafe work environment for staff and clients, inappropriate profile pictures, or information encouraging criminal activity.
- Unless it is program related, staff should limit the amount of bandwidth used. That includes streaming video and music, or downloading large files.
- Illegally downloading files is not allowed on our networks. This is to ensure the safety of our

servers and to respect copyright laws.

## **EMAIL USAGE**

Email is a vital way for communicating and sending information. As with the Internet section of the manual, the Companies seek to encourage email use in a safe and productive way. This section goes over how to access email, a few points on email etiquette, and email security. If staff have any questions, please contact the IT Department.

### **ACCESSING EMAIL**

Staff are able to access email through their work computer, and remotely using the Internet or Outlook application. The Companies assigned email should be used for business purposes only. No personal use is permitted.

- **DESKTOP APPLICATION**

Staff are able to access email on the Companies computers once they sign into the network. There is an Outlook icon on the desktop that can be clicked, or staff can search for the Outlook application.

- **OFFICE 365**

The Companies also uses Microsoft Office 365. This is a cloud-based system staff are able to use remotely. One of the many applications on Office 365 is webmail. Staff are able to check their email at any computer by signing into the portal or by going to office.com, clicking 'sign in,' and then entering in their email and password. Office 365 can be accessed on any PC, Mac, or mobile device.

- **OUTLOOK APP**

Staff can also check their email via their mobile devices by downloading the Microsoft Outlook app from their application store, not the mail app typically pre-installed on one's phone. If you have questions regarding the correct app to use, please contact the IT Department.

### **EMAIL SECURITY**

Staff encounter a good amount of email every day. The Companies use firewalls and anti-virus software to protect the network, but staff should be vigilant with email to ensure the network's safety. The following guidelines will help staff be prepared in case they receive email that may contain malware or look suspicious:

- Review the sender's email address. For example, if you receive an email from the President/CEO that seems out of place, look at the email address. If it is something that isn't close to the Companies' email address, please report the email using Phish ER or forward that email to the IT Department for review. Do not click on links or attachments in emails that are suspicious.
- If you are not familiar with the sender, do not open any attachments. They may contain a virus or malware. Please report the email using Phish ER or forward that email to the IT Department for review.
- A staff's email account may need to be accessed by an authorized member of the

Management Team or IT Department. That type of access will need to be authorized by their supervisor.

The Companies use an email filter to block or quarantine emails that could contain malware. To gain access to those emails, staff should sign on from the daily email that is from the email filter. The username and password are provided during orientation or can be reset by submitting a request in the portal.

- HIPAA guidelines must be followed. Do not send any Protected Health Information (PHI) that is unprotected.
- Staff should not distribute inappropriate content (outlined in the Internet Security section) via email. Any staff who receives an email they consider to be inappropriate should report the email to their supervisor or HR.

## **EMAIL ETIQUETTE**

The Companies cultivate a professional and friendly work culture. Email contributes to that culture. It is important that our electronic communications are respectful of other staff, their time, and storage space. The following are points that build on a positive culture:

- Use the 'important message' or 'high priority' setting only when needed. They should be used for messages that are important and require immediate attention and response.
- Try to use a meaningful subject line rather than leaving it blank, or using a single word like 'hello.'
- Please be mindful when using ALL CAPITAL LETTERS in messages or subject lines. This may be perceived as impolite, rude and could imply yelling or shouting.
- Staff's email signature should automatically be at the bottom of an email. Please do not remove the signature from the Outlook settings. Email signature must meet the New Hope standard.
- Please do not forward chain emails.
- Be sparing with group messages; only add recipients who will find the message genuinely relevant and useful.
- Avoid a case of the 'Reply-Alls' by inserting group email recipients in the 'BCC' (blind carbon copy) field. This eliminates unneeded 'reply-alls.' that clutter an inbox along with the risk others seeing information not meant for other staff.

## **Cell Phone Usage**

The New Hope Services cell phone policy offers general guidelines for using company cell phones. The purpose of this policy is to help us all get the most out of the advantages cell phones offer our company while minimizing distractions, accidents, and frustrations improper cell phone use can cause.

This policy applies to all New Hope Services employees who have been issued a company cell phone, or use a personal cell phone for work-related purposes. Staff approved to use their personal cell phone for work-related purposes may submit a PO to receive a monthly stipend. This stipend is provided to support work completed utilizing personal cell phones.

### **Cell Phone Use Guidelines**

The following are New Hope Services basic guidelines for proper cell phone use. In general, company cell phones should **only** be used for work.

- Never use a cell phone while driving.

- Never use a cell phone while operating equipment.
- Do not use cell phones for surfing the internet unless its work related.
- Do not download or play any games on company cell phone.
- Avoid using work cell phones for personal tasks.
- If Data is limited, avoid using data unless it's strictly work related.

We realize the cell phones can be great tools for our employees. We encourage employees to use cell phones for:

- Making or receiving work calls in the appropriate place and situation to do so.
- Other work-related communication, such as text messaging or emailing, in appropriate places and situations.
- Teams, FaceTime, or other video conferencing apps for work-related virtual visits or meetings.
- Scheduling and tracking of appointments.
- Carrying out work-related research.
- Tracking of work tasks.
- Tracking of work contacts.

#### **Virtual Meeting Guidelines:**

- While distractions are often unavoidable, try to keep them to a minimum. No music or television in the background during meetings.
- Keep yourself muted during video or audio conferencing unless you are speaking.
- Turning on video is encouraged but not required.
- Avoid eating a meal during a virtual meeting unless invited to do so by the meeting host.
- Casual dress is acceptable; however, use discretion. No sleeveless tops, pajamas or other apparel that would not be appropriate to wear to work (see Dress Code for details).
- Avoid multi-tasking. Give your full attention to the meeting as if you were face to face.

#### **Disciplinary Action**

Improper use of cell phones may result in disciplinary action. Continued use of company cell phones for personal use or in any other way that violates the guidelines of this policy, may lead to having cell phone privileges revoked.

Cell phone usage for illegal or dangerous activity, for purposes of harassment, or in ways that violate the company confidentiality policy may result in immediate termination.

### **HARDWARE/SOFTWARE USAGE**

The Companies' staff use hardware and software throughout each working day. Staff encounter both when printing/copying documents, inputting client notes, clocking in and out, etc. The IT department works hard to ensure staff are able to complete their jobs as smoothly as possible.

#### **HARDWARE**

Hardware is the physical technology: computers, phones, and copiers are considered hardware. When a staff member is hired, they are provided the necessary hardware according to their position and new hire form. Computers, and other pieces of technology valued over \$500 are assigned an Asset tag and are inventoried by the IT Department.

## **SOFTWARE**

Software is anything that is running on the hardware. From databases to email applications, staff use software to accomplish their tasks. When hired, each staff member is registered to the software according to their position. Each department has specific software that allows for program goals to be met. Some software is used extensively throughout the organization and is included in the IT Orientation. Links to frequently used software can be found in the 'Employee Resources' section of the Employee Portal (see The Companies' Portal section for more information).

## **NEW HOPE PORTAL**

The Portal is The Companies' intranet. Staff can access the portal by going to [www.newhopeservices.org](http://www.newhopeservices.org) and clicking the login link under the 'Employee' section of the menu bar. The Portal contains employee resources, news, and events that are used by staff in every department. Within the 'Employee Resources' section of the portal, staff can access links to frequently used software including, but not limited to, TimeWorks Plus, Relias, and Outlook webmail. Additionally, within the resource section, staff can access forms to request payments, process new hires, request maintenance or IT assistance, and create surveys. Organizational documents and manuals can also be found in the resource section.

## **PURCHASING HARDWARE/SOFTWARE**

If there is a need to acquire, replace, or upgrade any hardware or software, the Program Manager must get approval from EMT to submit a purchase request on the portal. The type of equipment purchased is based on best value to meet the performance objective. Any purchases must be in compliance with The Companies' Fiscal Policy.

Purchase requests should be submitted by the program manager through the portal in the 'Frequently Used' folder within the 'Employee Resources' section. Staff can also access the form by going to <https://www.newhopeservices.org/employee-resources/it-request-form/>

## **ASSISTANCE WITH IT ISSUES – SERVICE DESK**

If staff need assistance with hardware or software, they must submit a request on the portal using the *IT Request Form* as mentioned in the Purchasing section.

This form, once submitted, automatically creates a ticket. The IT department has a goal of closing out all requests within ten business days.

## **HARDWARE ACQUISITION/DISPOSAL/TRACKING**

### **HARDWARE\SOFTWARE PROCUREMENT**

All hardware and software procurement should start with a Help Desk ticket request. The IT Department will then assist with recommendations, pricing, testing, procurement and installation. This will aid in making sure the proper product is procured that will work with the current Companies network infrastructure. Any Hardware or Software equipment assigned to an employee will need to be signed for using our "Agreement to Return and Care for Company Equipment" form. If the employee has a need for a change of equipment, an IT request will need to be made using a new form.

## **HARDWARE\SOFTWARE DISPOSAL**

The hardware disposal process has multiple processes to ensure adequate destruction of data with certification if possible of the destroyed data, and proper disposal of the hardware.

Software disposal would be handled in the same manner to ensure complete destruction of data while following all applicable laws, guidelines, and industry recommended best practices.

## **HARDWARE\SOFTWARE TRACKING**

All hardware and software is tracked by installation of the Atera agent on Companies' workstations and laptops. It is imperative to maintain change control to ensure validity of our tracking controls. A log of all hardware that has been decommissioned and destroyed is maintained by the IT Department and kept on the file server. A report can be generated for all workstations and laptops as well as all companies' software at any time using this system.

## **DATA PROTECTION**

The safety of The Companies' IT infrastructure is vital to company's operations. The IT department manages data security for both internal and external functions.

### **INTERNAL ACCESS - DATA & TECHNOLOGY**

Physical access to critical technology and data is only accessible by IT personnel. The Commons and Gardner Place both use a VPN connection to access internal resources stored at the Center. This VPN is configured and controlled by firewall software at each individual location owned by the Companies.

### **EXTERNAL ACCESS - DATA & TECHNOLOGY**

External access to data and technology is handled in the following methods:

- **Firewalls** – Each New Hope owned facility is equipped with direct access and has a firewall installed to protect from external intrusions and to also configure and route network traffic internally and externally. All other network access is provided by the VPN.
- **VPN** – Staff who are permitted remote access to work remotely may utilize VPN software to connect to New Hope's systems. This will require a 2-Step authentication process. You will be required to enter your New Hope password for the first step and then using the FortiToken Mobile App you will be provided a PIN for validation.
- **Encryption** - The firewalls and VPN connection allow for data encryption to and from the end-user.

### **DATA BACKUP**

The Companies' servers and data are backed up each night. Carbonite online backup is used to maintain an off-site copy of data. The option for continuous backup is utilized so that the off-site data repository is updated when changes occur. Not all data can be accessed by Carbonite. In those cases, Datto backup service is used to make a complete copy of all server images on and off-site each day. VMWARE is used to host all server systems virtually. This allows an image of each server to be stored ensuring all operations may be restored in less than 24 hours.

### **DISASTER RECOVERY PREPAREDNESS**

WARE images can be used to restore IT services and data at any location that may have experienced a



disaster. All applications can be accessed remotely if necessary.

In the instance that networking equipment is damaged, destroyed, or malfunctioning, extra network switches, firewalls, will be obtained. New Hope also contracts for configuration and maintenance of all networking equipment, including firewalls.

If phone equipment is damaged, destroyed, or malfunctioning, we have a contract to assist if the IT department doesn't have the capability to abate the issue.

#### **OTHER SECURITY AREAS OF NOTE**

Users of The Companies' systems, network, internet, and email should adhere to the following principals:

- Staff should use secured email software to send protected and confidential data to **approved** sources. Unless otherwise notified, such data is not allowed to be physically taken or emailed outside The Companies' facilities.
- Staff will have annual training that covers the privacy of clients, PHI (Personal Health Information), confidentiality, email/network security and HIPAA Compliancy standards.

#### **MONITORING TECHNOLOGY USAGE**

Staff should use The Companies technology for program goals. There may be circumstances the call for the monitoring of employee technology. Any such intervention will only be carried out by authorized staff. Authorization will be granted through the program manager, in conjunction with the IT Manager, with approval of the EMT member that supervises said program.

Additionally, all technology used to access The Companies' network, systems, internet or email is part of The Companies' official records. The Companies may be legally compelled to provide that information to law enforcement agencies or other parties.

#### **POTENTIAL SANCTIONS**

Knowingly breaching these policies can put The Companies at risk and is a serious matter. Staff who do so may be subject to disciplinary action; up to and including termination. Employees and contractors may also be held personally liable for violating this policy.

Where appropriate, The Companies may involve the police or other law enforcement agencies in relation to breaches of this policy.

#### **RETURN OF COMPANY PROPERTY**

Any NHS property issued to you, such as keys, lap top computer, cell phone, or customer files, must be returned to NHS at the time of your resignation or dismissal, or whenever it is requested by your Supervisor or a member of management. You are responsible to pay for any property/equipment that you fail to return upon your separation from the company, or that is deemed to have been lost, stolen, or damaged as a result of misuse or neglect. You will be issued an invoice for the current fair market value of any property/equipment issued and not returned by the agreed upon date following your separation. You will be required to sign an agreement upon being issued company property/equipment. This agreement serves as your acknowledgement of financial responsibility.

Should you fail to return any company issued property/equipment, and further fail to tender payment for the invoice presented to you; this will be considered theft and may lead to criminal prosecution by the Company.

## **EMERGENCY ASSISTANCE**

In the case of an immediate need of assistance, please contact the IT Administrator or SVP/CFO. The contact info is:

### **Alex Sanders, IT Systems Administrator:**

Office: 812-288-8248 ext. 131

Mobile: 812-572-9263

Email: Alex\_Sanders@newhopeservices.org

### **John E. Broady, SR. VP/CFO:**

Office: 812-288-8248 ext. 129

Mobile: 502-931-3325

Email: CFO@newhopeservices.org