VILLAGE OF FREEPORT

Computer Use Policy

Version 5.0

APRIL 14, 2023

INCORPORATED VILLAGE OF FREEPORT
46 North Ocean Avenue Freeport, New York 11563

Village of Freeport Computer Use Policy

I. PURPOSE

Computer resources are provided by Freeport to employees and other authorized individuals to assist them with their work responsibilities and duties. Use of such resources is subject to a variety of laws, regulations and Village of Freeport policies.

The purpose of this policy is to outline the acceptable use of computer resources that all Village of Freeport employees and affiliates must adhere to. Appropriate organizational use of IT resources and effective security requires the participation and support of Freeport workforce ("users"). Inappropriate use of technology exposes Village of Freeport to potential risks including but not limited to virus attacks, compromise of network systems, servers and data, and legal liability.

Every Freeport computer and user is responsible for understanding and accepting these guidelines, and to conduct their activities accordingly. User adherence to this policy is an essential part of assuring that the technology resources are used only for intended purposes and will help mitigate the potential that inappropriate uses will expose Freeport to unnecessary risk.

II. SCOPE

This policy applies to all Freeport users of any systems, information or physical infrastructure including but not limited to desktop computers, mobile devices, email, internet, and telephony equipment used to support Freeport government entities. Therefore, this policy applies to any entity or person including employees (full-time and part-time), interns, consultants, vendors, contractors and guests who use Freeport computer resources and technology. It is every user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms.

III. ESSENTIAL FUNCTIONS

A. Department Heads

- Responsible for authorizing the use of Freeport technology resources.
- Responsible for defining approved Village business and network utilization practices.
- Responsible for communicating acceptable use policy (this policy) to their employees, including sign-off on Computer Usage Acknowledgement Form for new employee hires.
- Responsible for ensuring that all users within their department are adequately trained in the use of applicable hardware and software technologies.
- Departments that are subject to the Health Insurance Portability and Accountability Act (HIPAA) as a covered entity (health plans, healthcare clearinghouses, and/or providers that transmit any health related information in electronic form in connection with a transaction covered in the HIPAA transaction rule) are responsible for notifying the Information Technology Manager of this status to ensure that the Department's Privacy Officer and IT Security work with appropriate staff to ensure compliance with HIPAA security regulations.

- Departments that have electronically stored Personal, Private and Sensitive Information (PPSI) are responsible for notifying the Information Technology Manager to take appropriate steps to ensure that the information is maintained securely including the application of proper encryption and backup procedures.
- Shall notify the Executive Director of Human Resources of any suspected violation of this policy upon discovery.
- Shall work with the Executive Director of Human Resources and initiate the appropriate action to respond to violations of this policy.

B. Information Technology Center

- Coordinates requests for technology usage information that involves enterprise servers or enterprise application services for all authorized users.
- Facilitates appropriate utilization of external resources including civil or criminal investigators to examine suspected violations contained in stored data files and the Village's email system.
- Shall monitor departmental use of Freeport Computing Resources,
- May investigate excessive network traffic or bandwidth usage (high browser use or message volume) for improper use of Village of Freeport Technology Resources.
- Responsible for backing up copies of e-mail, audio, video and data files that are maintained and utilized by authorized Freeport personnel for legal, business, Freedom of Information Law (FOIL), or other reasons.
- Shall work with Freeport Departments that are covered HIPAA entities to assist with ensuring compliance with HIPAA security requirements and PPSI data security requirements.
- Shall review this policy periodically.
- Responsible for establishing and maintaining the vision, strategy and program to ensure information assets and technologies are adequately protected.
- Coordinates with Human Resource department on the development of internal policies, standards, guidelines and procedures for acceptable use.
- Responsible for establishing standards, guidelines and procedures to support this policy.
- Authorized to acquire and deploy the appropriate security tools necessary to ensure confidentiality, integrity and availability of Freeport's information system resources. Possession or use of security tools by other than specifically authorized IT staff is prohibited.
- Will report to Human Resource and Mayor's office any security risks, exposures or violations of this policy.
- May access a Freeport issued device without permission from the user or users both in person or remotely.

C. Authorized Computer Users

- Shall understand and abide by this policy.
- Shall understand that any login to or access of any Freeport Technology Resource constitutes their acknowledgement and acceptance of Freeport IT related policies.
- Shall use computer resources solely for their intended purposes.
- Must sign and submit an Acceptable Use Acknowledgement Form.
- Must declare their identity and declare their affiliation with Village of Freeport whenever Freeport Computing Resources are used.
- Should understand that using Freeport-provided equipment and software has no expectation of privacy in the use of these tools or any content.
- Shall keep all electronic communications professional and follow established practices regarding workplace professionalism.
- Responsible to protect and secure their Freeport Technology Resources from non-authorized or improper use.
- Responsible for following and adhering to the "use" restrictions of any external organization that they access or interface with.
- Shall immediately report any incident or violation to his policy to their Supervisor.
- Shall notify their Supervisor or IT support staff immediately should they suspect that their user account or data have been tampered with in any way.
- Shall report any computer, mobile device, or electronic media related HIPAA breaches to his or her Departmental Security Administrator and Privacy Officer who will ensure notification of the appropriate IT staff.
- Shall report any email that appears to be a scam with the Phish Alert Button in Outlook or contact the helpdesk directly @ext. 3606
- Shall be expected to save all of their work when they leave their computer.
- Shall be expected to store all files on a network drive. Any files that are lost due to being solely stored on a local drive is solely the fault of the user and cannot be recovered.
- Shall stay up to date on the current Computer Use Policy.
- Shall complete all Knowbe4 training within the timeframe designated in the notification.

IV. POLICY

A. General Guidelines

- Business Purpose, Acceptable Use and Expectation of Privacy:

- Village of Freeport Technology Resources are intended to be used for Village of Freeport business purposes with no expectation of privacy and are to be used to carry out the responsibilities associated with performance of Freeport employment; Freeport awarded contracts, or approved intergovernmental agreements.
- Authorized users shall not use Freeport computing resources for illegal, inappropriate, or obscene purposes, or in support of such activities. Use of Freeport Technology Resources for political or personal gain is also prohibited.
- Freeport uses software that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems.
- There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with Freeport equipment, email communications or Internet access. Accordingly, computer users should assume that whatever they do, type, enter, send, receive, and view on Freeport electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Freeport use at any time.
- Printing and copying should be kept to a minimum through the use of electronic media. When printing or copying is necessary, it should be done using printers and copiers that are capable of double-side printing.

- Incidental Personal Use:
  - Limited use of Freeport Computing Resources for personal needs is permitted as long as such use is consistent with any established Freeport department policy and union contract, and must not interfere or disrupt in any way other computer users, computer resources or Freeport services or equipment.

- Unacceptable Use:

  The following provides some examples of, improper uses of Freeport Computing Resources. Improper use of Freeport Computing Resources is not limited to these examples.

  - Pursues illegal activities such as anti-trust or libel/slander.
  - Violates copyrights (institutional or individual) or other license agreements (i.e. downloading or copying of data or software or music that is not authorized or licensed).
  - Knowingly, or with willful disregard, initiates an activity that disrupts or degrades network or system performance, or that crashes the network or other systems or that wastefully uses the finite Freeport computing resources.
  - Uses Freeport computing resources for fraudulent purposes.
  - Performs gambling activities or other illegal schemes (e.g. pyramid, chain letters, etc.).

- Steals intellectual property, data or Freeport computing resources.
- Misrepresents another user's identification (forges or acts as), or gains or seeks to gain unauthorized access to another user's account/data or the passwords of other users, or vandalizes another user's data.
- Views, retrieves, saves, or prints text or images of a sexual nature or containing sexual innuendo (i.e. accessing adult oriented sites or information via the Internet/Intranet).
- Invades systems, accounts, and networks to obtain unauthorized access to and/or to do damage (hacking). This includes unauthorized scans, probes, or system entries.
- Intentionally intercepts and modifies the content of a message or file originating from or belonging to another person or computer with the intent to deceive or further pursue other illegal or improper activities.
- Knowingly or with willful disregard propagates destructive programs into Freeport computing resources (i.e. worms, viruses, malware, Trojan horses, malicious code, email bombs, etc.).
- Uses Freeport computing resources to conduct commercial or private business transactions, or supports a commercial/private business other than Freeport business (i.e. using fax machines or telephones to further an employee's commercial/private business endeavors).
- Uses Freeport computing resources to access Internet video-streaming services such as YouTube, Netflix and Amazon for purposes not directly supporting Freeport business.
- Stores confidential information or private and sensitive information (see definitions and examples in Appendix) on a non-State Freeport issued device, or with a third party file storage service that has not been approved for such storage by the IT Department.
- Discloses protected Freeport data (confidential, private, or sensitive) via Freeport computing resources without proper authority.
- Any activity that promotes fundraising or advertising of non-Freeport organizations that have not been pre-approved by Freeport Mayor's Office is strictly prohibited.
- Generates or possesses material that is considered harassing, obscene, profane, intimidating or threatening, defamatory to a person or class of persons, or otherwise inappropriate or unlawful including such material that is intended only as a joke or for amusement purposes.
- Fails to comply with the instructions from appropriate Freeport staff to discontinue activities that threaten the operation or integrity of Freeport computing resources, or are deemed inappropriate, or otherwise violate this policy.
- Intentionally plagiarizes someone else's work whether that person works for Freeport or not.

- Intentionally or unintentionally trying to abuse any loop holes in Freeport's Computer Use Policy.
- Intentionally or unintentionally try to tamper with or disable any antivirus software.
- Uses another user's network or application account These users will be reported to Human Resources
- Users shall not use any Artificial Intelligence programs on Freeport issued devices

- Passwords and Authentication
  - Password Selection

    (1) The first line of defense to prevent an attack against Freeport's information systems is the use of strong passwords that meet certain complexity requirements. Users are to choose a password that meets the following minimum complexity requirements:

    - Cannot contain the user's account login name or parts of the user's full name that exceed two consecutive characters.
    - Minimum of 11 characters in length and must include all of the following requirements below:
      - Uppercase characters (A through Z)
      - lowercase characters (a through z)
      - Numbers 0 through 9 (multiple numbers can be used)
      - Special Characters (for example !, $, #, %)
    - Cannot use last 5 previous passwords.
    - May not include any part of the users name in the password

    Here is an example **ThankYou2021!** or Saf3Comput!ng

    (2) Enforcement. While it is the responsibility of the authorized user to select their password, Freeport reserves the right to enforce the use of passwords and their complexity by automated policy.
  - Password Security

    (1) Revealing account passwords to anyone or allowing use of an account by others is prohibited. This includes family and other household members when work is being performed remotely.
  - Password Aging

    (1) All users will be automatically required to change their passwords periodically -- at least once every sixty (60) days or less.
  - Tracking Previous Passwords Used

(1) Where software permits, a history file of passwords must be employed to prevent users from reusing passwords. The history file must minimally contain the last twelve (12) passwords for each user-ID.

- Password Storage

(1) For all Freeport information systems, passwords must be encrypted when stored or transmitted.

(2) Passwords must not be stored in unencrypted form in batch files, automatic login scripts, software macros, terminal function keys, computers without access control systems, or in other locations where unauthorized users might discover them. Similarly, passwords must not be written or produced in hard copy form and left in a place (i.e., a post-it note under the keyboard or next to the monitor screen) where unauthorized users might discover them.

- Limited Number of Log-in Attempts

(1) Access to an account will be locked-out if three unsuccessful login attempts occur during a preset time period. The number of allowable failed login attempts and the length of the lockout is dependent on the criticality of the system and the sensitivity of the information.

- Security
  - The IT Department will perform, at a minimum, the following tasks:

(1) Develop, deploy and maintain information security solutions that safeguard Freeport computer resources from intentional or unintentional harm.

(2) Provide support to Freeport Departments and computer users regarding security threats that could adversely affect Freeport computing and business operations and make recommendations to mitigate any associated security risks.

(3) Develop and promote security training and awareness programs that educate computer users on cyber-security risks and best practices.

(4) Support Incident Response activities, including forensic analysis when necessary.

(5) Engineer and deploy network defense countermeasures such as anti-virus, anti-spam and intrusion detection and prevention system solutions.

(6) Review and assess information security events and logs via sophisticated security information and event monitoring tools.

(7) Perform vulnerability assessments and penetration testing as necessary.

B. Software Installations and Licensing

- Freeport has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to

such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.

- Only approved Freeport standard software may be installed on computer resources and any transfer or copying of software in violation of applicable licenses or copyrights is prohibited and may lead to disciplinary action. The IT Department will be responsible for updating the catalog of standard software products and must be contacted before any software is installed on Freeport computer resources.
- Freeport mandates that effective licensing control and discovery measures are implemented to ensure compliance and minimize liability exposure.
- The IT Department will perform periodic assessment of software installed versus entitlements to ensure compliance with license agreements.
- Results of automated discovery will be reported to the departmental management upon completion to address any gaps requiring remediation.

C. Email Use

- Computer users must keep in mind that e-mail from Village of Freeport are visible representations of Freeport and that e-mail can be immediately distributed to unintended parties.
- Computer users must be cognizant that all written communications may be made public, monitored, reviewed and disclosed in litigation or other proceedings.
- All use of email must be consistent with Village of Freeport policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices in a professional and responsible manner.
- A Village of Freeport email account must be used for Village of Freeport business related purposes; personal communication is not permitted, Non-Village of Freeport related commercial uses are prohibited.
- Electronically stored Personal, Private and Sensitive Information (PPSI) may not be sent via email unless the data is sent via a password-protected encrypted method.
- Users must not transmit non-public, confidential, sensitive, or restricted information to or from personal email accounts (e.g., Gmail, Hotmail, AOl, Optonline, Verizon.net, Yahoo iCloud and others) or use a personal email account to conduct Freeport business unless explicitly authorized.
- Email should be retained only if it qualifies as a Village of Freeport business. Email is a Village of Freeport business record if there is a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a Village of Freeport business record shall be retained according to Village of Freeport Standard Operating Procedure Records Retention and Disposition Schedule MU-1, which provides instructions for managing public records in the custody of Village of Freeport Government.
- The Village of Freeport email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs/practices,

political beliefs, or national origin. Employees who receive any emails with this content from any Village of Freeport employee should report the matter to their supervisor immediately.

- Users are prohibited from automatically forwarding Village of Freeport email to a third party email system unless approved by a department head.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo and Microsoft to conduct Village of Freeport business, to create or memorialize any binding transactions, or to store or retain email on behalf of Village of Freeport. Such communications and transactions should be conducted through proper channels using Village of Freeport approved documentation.
- Using Village of Freeport resources for personal emails is Sending chain letters or joke emails from a Village of Freeport email account is prohibited.
- Village of Freeport authorized users shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- Village of Freeport non-employees are not permitted to use a Village of Freeport domain mailbox without management authorization.
- Personal Email Use. Use of personal email is strictly prohibited unless authorized for specific use by management and in writing. Violation of this policy by any user of IT resources may result in loss of access to those resources. Any Village employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

D. Internet Access

- The Internet is to be used to further Village of Freeport's mission, to provide effective service of the highest quality to Freeport's constituents and staff, and to support other direct job-related purposes.
- Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development
- Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.
- Accessing inappropriate content, as defined earlier in this policy document, is prohibited.
- Downloading unlicensed software or unauthorized sharing of Freeport data is prohibited.
- Freeport may impose restrictions, at the discretion of executive leadership, on the use of internet access and may block access to certain websites or services not serving legitimate business purposes. Such websites include but are not limited to:
    - Pornographic sites;
    - Sites that contain malicious content;
    - Most internet TV and radio sites;

- Social media (Facebook, Instagram, twitter, etc.)
- Dating websites
- Gaming and gambling sites.

- Village of Freeport authorized users shall have no expectation of privacy in anything they store, send or receive on the internet connection and there are automated controls in place to monitor user activity and to limit access to inappropriate content.

E. Use of Portable Storage Devices and Media Standard

For a variety of reasons, some individuals require the use of various portable storage devices and media in the course of performing their normal duties as an employee of the Village. The Information Technology Center currently provides these devices to individuals that have a legitimate need for such a device.

This section shall establish the Village standard regarding the acceptable use of these storage devices and media as well as the procedures for approving and monitoring their use

Personal Devices - The use of personal storage devices and media (i.e., those not purchased through the Village) of any form is expressly forbidden, unless explicitly authorized. This includes, but is not limited to the following:

- Portable Storage Devices
- Flash Media Cards/Drives, USB memory sticks, External Hard disk Drives
- Bluetooth Enabled Devices
- Internal/External CD and DVD Writers
- Writeable and rewriteable CD-ROMs and DVD-ROMs
- Notebook / Laptop, Desktop, tablet Computers and Smart phones
- Digital cameras, audio recording devices, portable music devices

Acceptable use of these devices for data storage - An employee's supervisor, Human Resources are responsible for approving the use of Portable Storage Devices to ensure that they are being used for legitimate business purposes.

Decommissioning Devices - In the event an employee leaves the Village, no longer has the need for such a device or has a device that is no longer functional, the device shall be returned to Information Technology Center. All data shall be removed or destroyed before a device is repurposed or destroyed. The employee's supervisor shall then ensure that the device is removed from the employee's record.

Process for Reporting Accidental Loss or Theft of such devices - The user shall take care not to lose the device or allow theft of the device. If the device/media is lost, stolen or otherwise rendered inoperable, the user shall contact their manager immediately. In the event of a lost or stolen device or media, the user shall disclose the nature of data/information that was stored on the device at the time of loss or theft at which time the manager will determine if any confidential information was involved

F. Computer Data Storage

Village employees may not save personal data including but not limited to documents, picture video files and or non-Village owned software on Village owned computers and prohibit such use altogether. If such data is found on Village owned equipment ITC will notify the user and remove any personal data immediately.

The Village Information Technology Center (ITC) will periodically review and will require that such data/software to be removed or relocated to network shared drives if it is hampering the function of the computer and the ability of the employee to perform his/her job function. In the event the employee gets a new computer or hard drive replacement, the Village will not be responsible for the restoration of any personal data. It is recommended that personal data is stored on external devices such USB/Firewire external drives which are to be purchased with personal funds and not connected to any Village computer unless approved by ITC.

The Desktop Support Specialist who is performing the data transfer or configuration will have discretion in identifying personal data. By default, only the Network drives will be backed up. Users requiring additional volumes or external drives that contain Village data to be backed up must specifically request this from their Desktop Support Specialist. Additionally, as a general guideline, files in My Pictures and My Music, including iTunes, will not be included in nightly backups nor will this data be transferred to a new hard drive. Users will assume responsibility for this transfer should it be desired. Please note that music, photographs, and videos used in Village work are exempt from this policy amendment.

G. Social Media

Steps for Departmental Use of Social Media

This section outlines what a Village department should do when using social media for official purposes. In summary, a department that is looking to use social media or that is already using social media should be sure that it follows the following steps for each use of social media (for example, go through the steps for the department's use of Facebook and separately for the department's use of Twitter):

- Consider whether and why it makes sense for your department to use the particular social media outlet
- Develop a Social Media Work Plan. Include
    - What Social Media Outlets you will use (Facebook, Twitter, LinkedIn, Other)
    - What type(s) of content you intend to post and promote via social media
    - How often you will post the content
    - Target audience for each type of content
    - Who will create the content
    - How you will promote the content

  - How you will track Success / Adjust Strategy if Needed
- Submit the Plan to the Mayor's office for review
- Designate department staff who will be responsible for the day-to-day use and maintenance of the service
- Create the social media presence for your department
- Make sure that department staff both routinely monitor the social media outlet and use the site for its intended purpose on a regular basis
- For any problems (such as people who post inappropriate content), work with the Mayor's office to address the problem
- Comply with the other requirements of this policy for the duration of the use of social media for official Village business
- Terminate use of social media outlet when the purpose has been fulfilled or the department is no longer using the site

Guidelines for Village Employees Who Use Social Media Outside of Work

These social media guidelines for Village of Freeport employees have been created to address some of the choices that individual employees, contractors, consultants, temporary staff and other workers at the Village may face online. These guidelines are not intended to address every situation encountered through use of a social media.

Whether or not a Village of Freeport employee chooses to create or participate in a blog, wiki, online social network or any other form of online publishing or discussion outside the workplace is his or her own decision. However, emerging online collaboration platforms are fundamentally changing the way Village employees work and engage with each other, clients and partners. The old social norms and standards still apply, but the openness of social media creates situations that call for new rules of etiquette.

Employee's personal use must not be attributable to the department or employee's job function at department. While an employee's use and comments made at social media sites are subject to First Amendment protections, as well as permissible restrictions, any personal use made of social media sites outside of work must not be attributable to the department or the employee's job function at the Village. For example:

- Do not use your work e-mail address to register for social media and other sites unless the purpose is directly related to your job.
- Do not display the Village of Freeport seal or other official Village logos, emblems or patches on personal social networking accounts.
- Don't provide the Village's or another's confidential or other proprietary information.

- Do not state or imply that you speak for the Village, for a Village department, or for Village officials.

Protect your privacy. Employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Village of Freeport is not responsible for the personal content of your social media sites. Be mindful that what you publish may be public for a long time. Be aware of your association with Village of Freeport in online social networks. If you identify yourself as a Village of Freeport employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and clients.

Use a disclaimer. Whether you publish to a blog or some other form of social media, make it clear that what you say there is representative of your views and opinions and not necessarily the views and opinions of Village of Freeport. Unless you are specifically authorized by your manager or supervisor to speak on behalf of the Village, consider including the following disclaimer on personal blogs or social media in which you identify yourself as a Village employee: "The postings on this site are my own and don't necessarily represent Village of Freeport's positions, strategies or opinions."

H. Wireless Telecommunications Devices (including personal devices)

- Department heads shall request the assignment of Freeport issued wireless telecommunications devices and/or services for employees on an as needed basis.
- All Freeport employees must abide by local laws, which prohibits the use of mobile devices during the operation of a motor vehicle without the use of hands free device.
- The Purchasing Director, or her designee, will place an order with a cellular service provider upon receipt of an authorization letter by a department head for Freeport issued devices.
- It will be the responsibility of the Purchasing and or IT Department to coordinate with the requesting department the delivery of Freeport issued wireless devices.
- Employees may use their personal electronic devices for work purposes when authorized by the employee's department head.
- In cases where the employees personal device needs to be configured or software installed, the employee must contact the Information Technology Center to arrange for the device to be configured based on Freeport-standards and to ensure that any Freeport-related information, including email and non-public data are stored in a secure and password-protected area.
- Employees may not use cloud-based applications or backup solutions that allow for Freeport-related data to be transferred to unsecure parties and personal devices may not be synchronized with other devices in employee's home.
- While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of Freeport issues equipment.
- Excessive personal calls, emails or text messaging during the workday for personal matters is prohibited.

- In order to prevent unauthorized access, personal devices accessing Freeport resources must be setup to auto-lock itself with a password or PIN if it is idle for more than 5 minutes.
- The employee's personal device may be remotely wiped or erased if the device is lost or if a data breach or virus is detected. Lost or stolen devices must be reported to the IT Department within 24 hours.
- While Freeport will take every precaution to prevent the employee's personal data from being lost in the event it must wipe a device, it is the employee's responsibility to take additional precautions such as backing up personal data including personal contacts.
- Freeport reserves the right to disconnect or disable services without notification to personal devices should activities warrant such action.
- The employee is personally responsible for all costs associated with his or her personal device and Freeport will not reimburse the employee for the cost of the device, monthly service charge, 3rd party application purchases or any other charges associated with the use of a personal device.

I. Portable Storage of Electronic Data

- Encryption is required as follows:
  - Freeport laptops and mobile devices that access or contain electronically stored Personal, Private and Sensitive Information (PPSI)
  - USB flash (thumb) drives or any portable media containing Freeport information, including but not limited to electronic PPSI
- Care must be taken when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of Freeport premises. User should never connect to unsecured public wireless networks.
- Equipment containing PHI or PPSI must be attended at all time or physically secured.

J. Acquisition and deployment of IT Resources

- All hardware and software acquisitions must conform to authorized standards in order to ensure appropriate technical support and assistance.
- All users must complete and sign a Village Assigned equipment form
- All hardware and software deployments and network connections must be performed by authorized IT personnel.
- All Freeport issued computer resources are the property of Freeport and when it's no longer required for any reason, the IT Department must be notified so the equipment can be properly disposed of including the elimination of all data stored to the device.

K. Virtual Private Network / Remote Access

A Virtual Private Network (VPN) is a secured private network connection built on top of a public network, such as the internet

- Security concerns associated with remote access include lack of physical security controls, the use of unsecured networks, the connection of infected devices to Freeport networks, the availability and storage of internal data to external devices, potential damage to Freeport resources and unauthorized access to Freeport information.
- All remote access must be requested by the Department Head and approved by the IT Department.
- Only approved employees and authorized third parties (outside agencies, vendors and contractors) can use remote connections to gain access to Freeport network resources.
- All computers that are connected to Freeport internal networks via remote access methods must be authorized by the IT Department and use the most up-to-date corporate standard anti-virus software.
- Remote access accounts are monitored by the IT Department and will be disabled after three consecutive months of inactivity. If remote access is subsequently required, the employee must request access as mentioned above.
- Remote access sessions must require re-authentication a period of inactivity and must not last more than 24 hours. All after hours business VPN access must be approved by a department head.
- Remote access users must ensure that their remote connections are treated with the same security standards as their on-site connection to Freeport network resources and data. When using non-Freeport issued devices for remote access, users must understand that their equipment are a de facto extension of Freeport network, and as such are subject to the same rules and regulations that apply to Freeport owned equipment and must take every reasonable measure to protect Freeport assets.
- Access to the Internet over Freeport remote access methods for recreational use is not permitted.
- It is the responsibility of all remote access users to ensure that remote connections are not used by unauthorized persons.
- All computer usage policies applicable at Freeport facilities also apply for use at remote sites
- Remote access users must never provide his or her login or password to anyone, not even family members.
- When remotely connected to Freeport network, a remote access user must ensure that his or her computer is not connected to any other network, with the exception of a personal home network.
- Information Technology Center is providing the VPN service and the service will be supported during 8:00a.m.–5:00p.m. business hours by the Network Operations

Center (NOC). After hours support will be handled by on-call personnel, but a response is not guaranteed until the next business day.

V. POLICY LIFECYLE MANAGEMENT

- This policy directive will be reviewed on an as needed basis but no less than annually by the Information Technology Center and Human Resources. Such review will include, but not be limited to, consideration of upgraded and new technologies, past experience with this policy directive and new and revised relevant legal requirements.

VI. Definitions

Acceptable Use: a use of Freeport computing or networking resources that is authorized and conforms to the acceptable use policy.

Village Approved Internet Service Provider (ISP): an internet service provider approved by the Information Technology Center.

Authorized Use: a use of Freeport computing or networking resources that is:

- Performed according to an employee's job description or as assigned by management to complete job goals.
- Performed according to a non-employee scope of work to complete contractual services for Freeport.
- Performed by a non-employee working for another municipality under an intergovernmental agreement (IGA) to accomplish services in the agreement for Freeport.

Authorized Computer User: all individuals approved to use in-scope computing and networking resources. This includes any entity or person including employees (full-time and part-time), interns, consultants, vendors, contractors and guests who use Freeport computer resources. (e.g. suppliers on contract or outside organizations with IGA's).

Computer Resources: items purchased or leased with Village of Freeport funds, or under the custody or control of Village of Freeport, including but not limited to, devices such as PC's, printers, telecommunications devices, mobile devices, servers and software applications. In addition, Computer Resources include all data and storage devices residing on the Village of Freeport network, including e-mail, as well as cloud computing and storage resources contracted for use for the benefit of Freeport.

Confidential Information: information that is available to an Authorized User only because of such user's position within Freeport and should be treated as confidential. Information does not have to be formally labeled "confidential" to be confidential, and must be protected from unauthorized disclosure or public release based on local, state or federal law. Examples include but are not limited to personally identifiable information such as name, address, phone number, social security number, bank account or credit / debit card number and protected health information. Also included as confidential information is Freeport intellectual property, security –sensitive infrastructure and operations information including without limitation design plans, blueprints, drawings and security protocols.

Department Heads: the Elected Official, Deputy Freeport Executive, Commissioner, or Department Director serving as the responsible party for conducting business on behalf of Freeport.

Electronic Protected Health Information (ePHI): Any protected health information (PHI) that is covered under the Health Insurance Portability and Accountability Act (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form. This includes

patient names, addresses, social security numbers, email addresses, fingerprints, photographic images, past medical records and payment information.

Email: the exchange of computer-stored messages by telecommunications means. Freeport standard email client is Microsoft Exchange 365.

Freedom of Information Law – (FOIL) New York State's Freedom of Information Law (Public Officers Law §87 et. Seq.) allows members of the public to access records of governmental agencies. FOIL provides a process for the review and copying of an agency's records.

HIPAA Privacy Officer: Oversees all activities related to compliance with federal regulations governing the privacy of health information. This includes the development, implementation, and maintenance of policies and procedures related to the privacy of and access to patient health information; and compliance with federal and state information privacy laws.

HIPAA Security Officer: is responsible for developing and maintaining the Department's security practices to meet HIPAA requirements. Responsible for protecting the Department's patients' ePHI from unauthorized access by working effectively with others to safeguard patient information.

IT Infrastructure: includes local and wide area networks (LAN and WAN), computing hardware (PCs and Servers), cloud computing and storage, communications hardware (including FAX, cell phones and desktop telephones), communications software (including protocol clients – i.e. FTP, web browsers, etc.), and remote access and data distribution technologies.

Improper Use: use of Freeport computing or networking resources for illegal, inappropriate, obscene, political, or personal gain purposes.

- Illegal activity is defined as a violation of local, state, and/or federal laws.
- Inappropriate use is defined as a violation of the intended use of the IT Infrastructure and Freeport Computing Resources and/or purpose and goal.
- Obscene activity is defined as a violation of generally accepted social standards for use of a publicly owned and operated communications vehicle.

Network: a system of interconnected Freeport Technology Resources designed to facilitate the sharing of devices and information among local and remote electronic systems used by authorized users.

Social Media: utilizes mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create, discuss and modify user-generated content, such as Facebook, Twitter, LinkedIn, YouTube, Google+, Flickr, Tumblr, Instagram, Pinterest, Snapchat.

Personally Identifiable Information: information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personal, Private and Sensitive Information (PPSI): information that is generally used internally within Freeport or with its authorized partners. Information that if lost, compromised, or disclosed to an unauthorized party could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual or the reputation of Freeport.

Technology Resource: any computing device, peripheral, software, information technology (IT) infrastructure, electronic data or related consumable (e.g. paper, disk space, central processor time, and network bandwidth) owned or controlled by Freeport.

5. Related Standards, and Forms

- Village Assigned User Equipment Form

Village of Freeport Assigned User Equipment

I, **<insert name>**, in my capacity as an employee of Village of Freeport, I have been trusted with certain equipment to assist me in my job responsibilities, I understand and confirm that this equipment including software is the sole and exclusive property of Village of Freeport.

Listed below is the equipment that has been assigned to me:

Equipment Type, Model and Accessories	Serial Number

I also agree to the following:

1. To take proper care of the equipment.
2. Not to check the equipment as luggage when traveling.
3. Not to **install** or **uninstall** any kind of software or to change the System Configuration without the consent and guidance of the IT Department.
4. To take full responsibility for any repairs or time spent reconfiguring the equipment, due to negligence on my part.

By my execution hereof, I hereby agree to forthwith return all aforesaid equipment, in good order and condition, to Village of Freeport., if my employment terminates for any reason whatsoever and in the event that I fail to do so, Village of Freeport., is hereby authorized and instructed to deduct the original cost of the same, from any amounts due to me.

_____ _____

Employee Signature Date

_____ _____

ITC Department Representative Date

CC: HR/Payroll Department

VII. REVISION HISTORY

Date of Change	Responsible	Summary of Change
March 1, 2018	ITC	Creation of New Policy
April 6, 2018	ITC	Updated and converted to new format
April 12, 2018	Engineering	Comments to Document
April 12, 2018	ITC	Changes made to document
May 9, 2018	ITC	Change made to desktop section
May 10, 2019	ITC	No Changes Made
May 1, 2020	ITC	No Changes Made
April 1, 2020	ITC	Updated Password Policy, Email Provide Update
April 1, 2021	ITC	No Changes
May 1, 2022	ITC	Updated Personal Data on Computers
August 1, 2023	ITC	Updated Personal Emails and AI.

VIII. COMPUTER USE ACKNOWLEDGEMENT FORM

I have received a copy of the Village of Freeport Computer Use Policy, which sets forth the acceptable and prohibited uses of Freeport computer resources.

By signing the document below, I acknowledge receipt of, and agree that I have read and understand the policies as set forth in this Policy.

In addition, I am aware that I have no expectation of privacy with respect to e-mail messages, internet usage or any other use of Freeport computer resources and such use may be monitored, intercepted, recorded, read, copied, accesses or captured in any manner including real time, and used or disclosed in any manner by authorized personnel with prior notice to individuals.

I further understand that a violation of this Policy may result in disciplinary action up to and including termination of employment as well as the imposition of any available civil and criminal sanctions.

_____

Name

_____ _____

Signature Date