VILLAGE OF HASTINGS-ON-HUDSON

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

Appropriate organizational use of information technology (IT) resources and effective security require the participation and support of the Village workforce ("users"). Inappropriate use exposes the Village to potential risks including virus attacks, compromise of network systems and services, and legal issues.

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the Village's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to all computer files and all forms of electronic communication, including email, text messaging, instant messaging, telephones, computer systems and other electronic records. In addition to the notice provided in this policy, users may also be notified about this monitoring and reminded that unauthorized use of the Village's IT resources is not permissible through the use of warning banner text at system entry points where users initially sign on.

The Village may impose restrictions, at its discretion, on the use of a particular information technology resource. For example, the Village may block access to certain websites or services not serving legitimate business purposes or may restrict users' ability to attach devices to the Village's information technology resources (e.g., personal USB drives, iPods).

Acceptable Use

All uses of information technology resources must comply with Village policies, standards, procedures, and guidelines, as well as any applicable Federal, State and local laws, including copyright laws and licensing agreements.

Consistent with the foregoing, acceptable use of information technology resources encompasses the following duties:

- Protection of confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved information technology devices or services; and
- Immediately reporting suspected computer security incidents to the Village Manager and the Information Technology Director.

Unacceptable Use

The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during the course of their authorized job responsibilities, after approval from Village Manager, in consultation with the Technology Director (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes the following:

- Distributing, transmitting, posting or storing, any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate or accessing or visiting a website containing such material;

- Purporting to represent the Village in matters unrelated to official authorized job duties or responsibilities;

- Connecting unapproved devices to the Village network or any State information technology resource;

- Connecting Village information technology resources to unauthorized networks;

- Connecting to any wireless network while physically connected to a Village wired network;

- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with Village policies;

- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (employees must recognize the inherent risk in using commercial email services as email is often used to distribute malware);

- Using Village information technology resources to circulate unauthorized solicitations or advertisements for non-Village purposes including religious, political, or not-for-profit entities;

- Using the computer system to copy and/or transmit any software programs, documents, or other information protected by the copyright laws;

- Providing unauthorized third parties, including family and friends, access to the Village IT resources and facilities;

- Using Village information technology resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside

employment or business activity (e.g., consulting for pay, business transactions);

- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using Village information technology resources; and
- Tampering, disengaging or otherwise circumventing Village or third-party IT security controls.

Occasional and Incidental Personal Use

Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy, is limited in amount and duration, and does not impede the ability of the individual or other users to fulfill the Village's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. The Village Manager may revoke or limit this privilege at any time.

For example, employees may make occasional and incidental personal use of information technology resources during their scheduled lunch and work break. Under no circumstances should personal use interfere with their regular work responsibilities.

Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgment by providing the above guidelines. If you are unclear about the acceptable "personal" use of a Village-provided resource, seek authorization from your immediate supervisor.

Individual Accountability

Security of the Village's computer system is a top priority. Employees and Authorized Users must have a unique user ID and password to protect against unauthorized access to files on which they are working. (Note that individual passwords do not prevent authorized Village representatives from accessing those files.)

Individual accountability is required when accessing all IT resources. Each individual is responsible for protecting against unauthorized activities performed under his/her user ID. This includes locking your computer screen when you walk away from your system and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure, including sharing. Credentials must be treated as confidential information and must not be disclosed or shared.

Users are never permitted to utilize another user's account without express permission of that account holder. Any attempt to log-on to the network as a system administrator may result in cancellation of user privileges and/or discipline. Any employee or authorized user identified as a security risk may be denied access to the network.

E-mails or other messages may not be sent in such a way that they appear to have originated with someone else. Log-on and other passwords may not be shared with any third party, and they may not be shared with other Village employees, except when authorized by a Supervisor or Department Head.

Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit non-public, confidential, sensitive, or restricted Village information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct Village business unless explicitly authorized. Users must not store non-public, confidential, sensitive or restricted Village information on a non-Village issued device, or with a third-party file storage service that has not been approved for such storage by the Village Manager.

Confidential Information

All Village information should be treated as confidential information. Employees and Authorized Users must exercise a greater degree of caution in transmitting Village information that exists in electronic form, including customer-related information, on the computer network. Confidential information should never be transmitted or forwarded to individuals inside or outside the Village or to companies who are not authorized to receive such information. Employees and Authorized Users are expected to use care in addressing messages (including emails, facsimiles, voice mail messages, and text messages) to make sure that such messages are not inadvertently sent to an unauthorized user or entity either inside or outside of the Village.

Individuals using distribution lists should take measure to ensure that the lists are current. Do not forward messages containing confidential information to multiple parties unless there is a clear business need.

Confidential information must not be displayed on a user's computer when the computer is left unattended. When computers are left unattended, they must be set to "locked" status with the password protected screen saver on, until the user returns. Diskettes, CDs, flash-drives, external hard-drives, or other removable media that contains confidential Village information must not be left open to access by unauthorized persons and should be kept in locked drawers or file cabinets.

Extra precautions must be exercised when taking confidential information out of the office in a laptop computer or PDA-type device. Users must never leave laptop computers or other portable devices that contain confidential information unattended when traveling. Caution should be used with Infrared transmitters on laptops and PDAs so that information is not accidentally passed to nearby laptop computers or other handheld devices.

User Responsibility for Information Technology Equipment

Users are routinely assigned or given access to information technology equipment in connection with their official duties. This equipment belongs to the Village and must be immediately returned upon request or at the time an employee is separated from the Village. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the Village. Should Village IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances

surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The Village has the discretion to not issue or re-issue information technology devices and equipment users who repeatedly lose or damage Village IT equipment.

Revised 10/4/2019