Information Technology Use

321.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of department information technology resources, including computers, electronic devices, hardware, software and systems.

This policy does not supersede, but supplements any related Village information technology policy.
See attachment: Grafton IT Policy_2017_final_.pdf

321.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the Grafton Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

321.2 POLICY

It is the policy of the Grafton Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

321.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history made at any department computer or over any department network. The fact that access to a database,

service or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices or networks.

The Department will not request or require, as a condition of employment, that employees disclose access information for their personal Internet accounts or otherwise grant access to, or allow observation of, those accounts unless specifically permitted to do so under federal or Wisconsin law (Wis. Stat. § 995.55).

321.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to the Platoon Sergeants.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

321.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any department computer. Members shall not install personal copies of any software onto any department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the Assistant Chief of Police or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of department- or Village-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from administration and a full scan for malicious attachments.

321.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law

enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

321.4.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information shall be limited to messages, mail and data files.

321.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other "off the clock" work-related activities. This also applies to personally owned devices that are used to access department resources.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

321.5 PROTECTION OF AGENCY SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by administration and shall be changed at intervals as directed by administration.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

321.6 INSPECTION OR REVIEW

Administration or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by administration or during the course of regular duties that require such information.

Attachments

Grafton IT Policy_2017_final_.pdf

VILLAGE OF GRAFTON

INFORMATION TECHNOLOGY POLICIES

Contents:

PURPOSE:

To better serve our citizens and give our workforce the best tools to do their jobs efficiently, the Village of Grafton (the "Village") continues to adopt and make use of new means of communication and information exchange. This means that many of our employees have access to one or more forms of electronic media and services, including, but not limited to, computers, e-mail, telephones, cellular telephones, pagers, voice mail, fax machines, external electronic bulletin boards, wire services, on-line services, and the Internet,.

The Village encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information. However, all electronic media and information technology resources (i.e. equipment, Email/Internet access, etc.) provided by the Village are Village property and their purpose is to facilitate and support Village business with no expectation of privacy on behalf of employees or those connected with the Village. Moreover, it is to be understood that certain electronic records are considered public record under State of Wisconsin law and can be subject to open records requests.

These policies cannot lay down rules to cover every possible situation. By adopting these policies, it is the Village's intent to ensure the Village's information technology resources are used to their maximum potential for business purposes and not used in a way that is disruptive, offensive to others, or contrary to the best interest of the Village.

ORGANIZATIONS AFFECTED:

These policies apply to all Village of Grafton departments, offices, boards, commissions, committees, Village employees and contracted and consulting resources.

SECTION 1 – ELECTRONIC EQUIPMENT & SERVICES

1.1 The following policies apply to all electronic media and services that are:

- Accessed on or from Village premises;
- Accessed using Village –owned equipment or via Village-paid access methods; or
- Used in a manner that identifies the individual as acting for or on behalf of the Village; or in anyway identifies the Village.

1.3 POLICY:

It is the policy of the Village to follow this set of procedures for the use of electronic communication media and services.

1.4 REFERENCES:

Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510 – 2711); Wis. Stats. §947.0125.

1.5 PROCEDURES:

1.5.A ACCESS and AUTHORITY

1) Each Department Head shall determine which employees in their department shall have access to the various media and services, based on business practices and necessity and which shall have authority to communicate on behalf of the Village.
2) The provisions of this Policy shall apply to the use of Village-owned/provided equipment and/or services from home or other locations off Village premises. Village-owned equipment (e.g. lap tops, cellular telephones, etc.) may be removed from Village premises solely for Village work related purposes pursuant to prior authorization from the Department Head.
3) New users, as soon as practical after hire, shall attend training to be educated about the risks of information disclosure and be made aware of various attack mechanisms (i.e. virus, malware, etc.).
4) Users shall change their network passwords every sixty (60) days to help ensure their login credentials remain secure.

1.5.B PROHIBITED ACTIVITIES

1) Electronic media cannot be used for knowingly transmitting, retrieving or storing any communication that is:

   a) Personal business on Village time (e.g. sports pools, games, shopping, correspondence or other non-business-related items/documents), except as otherwise allowed under Section 1.5.C;
   b) Discriminatory or harassing;
   c) Derogatory to any individual or group;
   d) Obscene as defined in Wis. Stats.;
   e) Defamatory or threatening; or
   f) Engaged in for any purpose that is illegal or contrary to the Village's policy or business interests.
   g) Intentional misrepresentation of official village policy in any message posted to the Internet.

2) For the protection, integrity and security of the Village's System, electronic media shall not be used to download or transfer software, unless authorized by the Village Administrator.

3) Unless it is a part of your recognized job duties, employees are not to make changes to either software and/or hardware configurations on village-owned equipment.

1.5.C PERSONAL USE

1) Except as otherwise provided, electronic media and services are provided by the Village for employees' business use during Village time. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal non-business purposes is permitted as set forth below:

a) Personal use is limited to breaks, lunch or within 30-minutes before/after work;
b) Personal use must not interfere with the productivity of the employee or his or her co-workers;
c) Personal use does not involve any prohibited activity (see Section 1.5.B);
d) Personal use does not cause network congestion, consume system resources or storage capacity on an ongoing basis;
e) Personal use does not involve large file transfers or otherwise deplete system resources available for business purposes.
f) Personal use does not pose nor create any security risks for the system.
g) Personal use does not cause either physical damage to the equipment or corruption/malfunction due to malware/virus attack.

2) Village telephones and cellular phones are to be used for Village business. However, brief, limited personal use is permitted during the work day. Personal long distance calls are only permitted with the use of a personal 1-800 calling card, or with the understanding that such calls must be reimbursed to the Village, as per policies set forth in the Village Employee Personnel Manual.

3) Employees should not have any expectation of privacy with respect to personal use of the Village's electronic media or services.

1.5.D ACCESS TO EMPLOYEE COMMUNICATIONS

1) The Village respects its employees' desire to work without surveillance. However, electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, Internet, text messages and bulletin board systems, desktop faxes, and similar electronic media may be accessed and monitored by the Village.

2) The Village reserves and intends to exercise the right, at its discretion, to review, monitor, intercept, access and disclose all messages created, received or sent over the electronic communication systems (i.e. computer, cellular telephone, etc.) for any purpose including, but not limited to: cost analysis; resource allocation; optimum technical management of information resources; and detecting use which is in violation of Village policies or may constitute illegal activity. Disclosure will not be made except when necessary to enforce the policy, as permitted or required under the law, or for business purposes.

3) Any such monitoring, intercepting and accessing shall observe any and all confidentiality regulations under federal and state laws.

1.5.E SECURITY/APPROPRIATE USE

1) Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the Administrator's Office, employees are prohibited from engaging in, or attempting to engage in:

   a) Monitoring or intercepting the files or electronic communications of other employees or third parties;
   b) Hacking or obtaining access to systems or accounts they are not authorized to use;
   c) Using other people's log-ins or passwords; and
   d) Breaching, testing, or monitoring computer or network security measures.

2) No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

3) Electronic equipment and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

4) Anyone obtaining electronic access to other organizations', business', companies', municipalities' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner.

5) Employees must understand that the unauthorized use or independent installation of non-standard software or data may cause computers and networks to function erratically, improperly, or cause data loss. Therefore, before installing any new software or data, users should seek the assistance of the Village Administrator. Users must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

6) Most of the Village's computing facilities automatically check for viruses before files and data which are transferred into the system from external sources are run or otherwise accessed. On computers where virus scanning takes place automatically, the virus scanning software must not be disabled, modified, uninstalled, or otherwise inactivated. If you are uncertain as to whether the workstation you are using is capable of detecting viruses automatically, or you are unsure whether the data has been adequately checked for viruses, you should contact the Village Administrator.

7) Anyone receiving an electronic communication in error shall notify the sender immediately. The communication may be privileged, confidential and/or exempt from disclosure under applicable law. Such privilege and confidentiality shall be respected.

1.5.F ENCRYPTION

Employees should not assume electronic communications are totally private. Employees with a business-need to encrypt messages (e.g. for purposes of safeguarding sensitive or confidential information) shall submit a written request to the Village Administrator.

When authorized to use encryption, employees shall use encryption software supplied to them. Employees who use encryption on files stored on a Village computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

1.5.G PARTICIPATION IN ON-LINE FORUMS

1) Employees should remember that any messages or information sent on Village-provided facilities to one or more individuals via an electronic network (for example: Internet mailing lists, bulletin boards, and on-line services) are statements identifiable and attributable to the Village.

2) The Village recognizes that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a newsgroup devoted to the technical area.

3) Employees shall include the following disclaimer in all of their postings to public forums:

> "The views, opinions, and judgments expressed in this message are solely those of the author. The message contents have not been reviewed or approved by the Village of Grafton."

4) Employees should note that even with a disclaimer, a connection with the Village exists and a statement could be imputed legally to the Village. Therefore, employees should not rely on disclaimers as a way of insulating the Village from the comments and opinions they contribute to forums. Instead, employees must limit their discussion to matters of fact and avoid expressing opinions while using the Village's systems or Village provided account. Communications must not reveal confidential information and must not otherwise violate this or other Village policies.

5) Employees must receive authorization from their Department Heads prior to participating in an on-line forum. The employees shall be required to review the provisions of this section before they receive such authorization.

SECTION 2 - E-MAIL POLICY

2.1 POLICY:

It is the policy of the Village to follow this set of procedures for the use of the Village's e-mail system.

2.2 REFERENCES:

Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510 – 2711); Wis. Stats. §19.21; Wis. Stats. §947.0125.

2.3 PROCEDURES:

2.3.A ACCESS TO EMPLOYEE E-MAIL

1) Employees should not have any expectation of privacy with respect to messages or files sent, received, or stored on the Village's e-mail system. E-mail messages and files, like other types of correspondence and Village documents, can be accessed and read by authorized employees or authorized individuals outside the Village. The Village reserves the right to monitor, review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system. Information contained in the e-mail system will only be disclosed to the extent permitted by law, for business purposes, or as needed to enforce the policy. Authorized access to employee e-mail by other employees or outside individuals includes, but is not limited to, the following:

   a) Access by the Village Administrator's Office during the course of system maintenance or administration;
   b) Access approved by the employee, the employee's supervisor, or an officer of the Village when there is an urgent business reason to access the employee's mailbox - for example, if an employee is absent from the office and the supervisor has reason to believe that information relevant to the day's business is located in the employee's mailbox;
   c) Access approved by the employee's supervisor, the Village Administrator, or an officer of the Village when there is reason to believe the employee is using e-mail in violation of the Village's policies;
   d) Access approved by the Village Administrator or the Village Attorney in response to the Village's receipt of a court order or request from law enforcement officials for disclosure of an employee's e-mail messages.

2) Except as otherwise noted herein, e-mail should not be used to communicate sensitive or confidential information. Employees should choose a more secure method for the transmittal of information deemed sensitive or confidential. Employees should anticipate that an e-mail message might be disclosed to or read by individuals other than the intended recipient(s), since messages can be easily forwarded to other individuals. In addition, while the Village endeavors to maintain the reliability of its e-mail system, employees should be aware that a variety of human and system errors have the potential to cause inadvertent or accidental disclosures of e-mail messages.

3) The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

4) Employees should understand that electronic mail is a written form of communication, just like a paper letter. Though electronic mail is relatively spontaneous compared with regular mail, employees should take care to use the same level of discretion and forethought before executing electronic messages.

2.3.B PASSWORDS

Each user accesses the e-mail system by means of a personal log-in name and password, which will be selected by the employee and kept on file with their respective Department Head.

1) Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. From a systems perspective and from the perspective of an e-mail recipient, passwords also establish the identity of the person sending an e-mail message. The failure to keep passwords confidential can allow unauthorized individuals to read, modify, or delete e-mail messages; circulate e-mail forgeries; and download or manipulate files on other systems.

2) The practice of using passwords should not lead employees to expect privacy with respect to messages sent or received. The use of passwords for security does not guarantee confidentiality.

3) Passwords should never be given out over the phone, included in e-mail messages, posted, or kept within public view.

4) Employees are prohibited from disclosing their password, or those of any other employee, to anyone who is not an employee of the Village. Employees also should not disclose their password to other employees, except when required by an urgent business matter.

2.3.C SECURITY AND APPROPRIATE USE

1) Personal use of the Village's e-mail system is not permitted.
   a) Incidental personal messages shall be deleted as soon as they are read or forwarded to an employee's personal account.
   b) Employees should not store copies of the personal messages on the Village network.

2) Personal Email accounts may only be accessed on Village-owned equipment in accord with Section 1.5 C above:
   a) Employees should not have any expectations of privacy with respect to personal e-mail sent or received on Village equipment.
   c) Village and departmental management reserve the right to examine at any time and without prior notice, all E-mail directories, files and other information stored on Village-owned data disks, computers, or tape.

3) Virus infections are one of the well-documented threats of Email usage. It is important that employees scan all incoming messages for possible viruses. Users should not open or attempt to read any files attached to electronic mail messages that are not readily identifiable or that they did not specifically request and should immediately contact their Department Head and/or the Village Administrator upon receiving an unrequested file.

2.3.D PROHIBITED ACTIVITIES

1) Employees are strictly prohibited from sending e-mail or otherwise using the Village's e-mail system in connection with any of the following activities:

a) Engaging in personal business or entertainment on Village time;
b) Engaging in illegal, fraudulent, or malicious activities;
c) Engaging in the unlawful use of the e-mail system as set forth in Section 947.0125 of the Wisconsin Statutes (Unlawful use of computerized communication systems);
d) Sending or storing offensive, disruptive, obscene, or defamatory material. Materials which are considered offensive include, but are not limited to: any materials which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, race, creed, color, sex, ancestry, religious or political beliefs, marital status, national origin or disability;
e) Annoying or harassing other individuals;
f) Using another individual's account or identity without explicit authorization;
g) Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
h) Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization from the Finance Department; or
i) Permitting any unauthorized individual to access the Village's e-mail system.

2.3.E CONFIDENTIAL INFORMATION

1) All employees are expected and required to protect the Village's confidential information. Employees shall not transmit or forward confidential information to outside individuals or companies without the permission of their supervisor. See Section 2.5.G, Encryption.

2) The Village also requires its employees to use e-mail in a way that respects the confidential and proprietary information of others. Employees are prohibited from copying or distributing copyrighted material - for example, software, database files, documentation, or articles - using the e-mail system.

SECTION 3 – ELECTRONIC RECORD RETENTION POLICY

3.1 POLICY:

All electronic information created or communicated by an employee using email, voicemail, telephones, text messages, Internet access and computer files may be accessed and monitored by the Village. The Village reserves the right, at its discretion, to review, monitor and disclose all messages and files created, received or sent over electronic communication systems as required. It is the policy of the Village to follow this set of procedures for record retention.

3.2 REFERENCES:

Wis. Stats. §§16.612, 19.21 et. seq., 19.32 and 19.33.

3.3 PROCEDURES:

3.3.A NATURE OF ELECTRONIC RECORDS

As a general rule, an electronic record is a public record whenever a paper message with the same content would be a public record. See Wis. Stats. §19.32(2) for definition of a record.

3.3.B COMPONENTS OF AN E-MAIL RECORD

In particular, an e-mail record is defined to include the message, the identities of the sender and all recipients, the date, and any non-archived attachments to the e-mail message. Any return receipt indicating the message was received by the sender is also considered to be part of the record.

3.3.C SAVING AND INDEXING RECORDS

Initially the custodian (that officer, department head, division head, or employee of the Village who keeps or is in possession of a record) bears the responsibility for determining whether or not a particular electronic record is a public record which should be saved and ensuring the record is properly indexed and forwarded for retention as a public record. E-mail which is subject to records retention must be saved and should be indexed so that it is linked to the related records in other media (for example, paper) so that a complete record can be accessed when needed. E-mail records to be retained shall be archived to an achievable media, network drive or printed out and saved in the appropriate file. Any officer, department head, division head, or employee of the Village may request assistance from the Legal Custodian of records (the Village Clerk or the Clerk's designee, except that the Chief of Police is Legal Custodian of Police Department records) in determining whether an e-mail is a public record.

1. RESPONSIBILITIES FOR E-MAIL RECORDS MANAGEMENT

a) Legal Custodian. E-mail records of a Village authority having custody of records shall be maintained by the designated Legal Custodian, pursuant to Village policy.

b) Information Services Manager. If e-mail is maintained in an on-line database, it is the responsibility of the Village Administrator to provide technical support for the Legal Custodian as needed. When equipment is updated, the ability to reproduce e-mail in a readable form shall be

maintained. Village e-mail programs shall be properly set up to archive e-mail.

2. PUBLIC ACCESS TO E-MAIL RECORDS

If a Department receives a request for release of an e-mail public record, the Legal Custodian of the record shall determine if it is appropriate for public release, in whole or in part, pursuant to law, consulting the Village Attorney, if necessary. As with other records, access to or electronic copies of disclosable records shall be provided within a reasonable time through the same procedure as requests for public record..

SECTION 4 – INTERNET ACCESS POLICY

4.1 POLICY:

It is the policy of the Village to follow this set of procedures for access to the Internet via the Village's network.

4.2 GOVERNING INTERNET ACCESS BY EMPLOYEES:

(a) The Village may provide access to the Internet for some employees. This capability will be provided on an "as needed" basis and is a revocable privilege. Before being granted Internet access, each employee must sign an agreement that they will comply with all of the requirements of this Policy.

(b) All internet access may be monitored and logged at any time without notification. Those logs may be made available at the request of management, Village officials or by Village Attorney in regards to an Open Records Request.

(c) The Village reserves the right to block access to certain websites it deems appropriate.

(d) Access to some resources requires that an additional fee be paid. Department head or supervisors should require that staff seek prior approval for access to any fee-based Internet resources.

(e) When employment terminates or an employee assumes a new position or responsibilities, his/her Internet authorization must be reviewed for continued access. Access termination is accomplished by departmental notification to the Village Administrator.

(f) Each individual is responsible for complying with all applicable state and federal laws, and all village policies and standards when accessing the Internet. Violations of any policies or standards can result in disciplinary action in accordance with village rules. Abuse of Internet access by individuals can result in the revocation of Internet privileges for the entire department.

4.3 SECURITY AND APPROPRIATE USE

(a) Village Internet Access shall primarily be for Village business. Internet transmissions sent from or received by village computers are considered village property.

(b) Personal Use may only be allowed in accord with Section 1.5 C). The restrictions listed shall apply.

(c) Virus infections is one of the well-documented threats of Internet use. It is important that employees scan all incoming files for viruses, whether downloaded or attached to electronic mail messages. Users should not open or attempt to read any files or viruses, whether downloaded or attached to electronic mail messages. Users should not open or attempt to read any files received over the Internet that they did not specifically request and should immediately contact their Department Head and/or the Village Administrator upon receiving an unrequested file.

SECTION 5 – POLICY VIOLATIONS

5.1 Progressive Discipline for Policy Violations

(a) It is recognized that inadvertent user errors can occur where an "infected" web link, Email message, or message attachment are opened which in turn causes damage to either the work station and/or the Village network. The Village's intention is to properly train its employees on how to avoid such circumstances.

(b) In the event that repeated violations of this policy occur through deliberate irresponsible use of Village equipment and network the following progressive discipline up to and potentially including termination may be applied:

a. 1st occurrence: Mandatory training.
b. 2nd occurrence: Verbal warning and mandatory training
c. 3rd occurrence: Written warning, mandatory training, and potential for reimbursement by the employee for the I.T. support costs related to remedying the problem/damage caused.

INFORMATION TECHNOLOGY POLICIES

EMPLOYEE NOTICE

As an employee of the Village of Grafton (the "Village"), I recognize and understand that the Village's information technology resources are provided for conducting the Village's business in a cost effective and efficient manner. However, Village policy does permit some very limited, occasional, or incidental personal use of the equipment and services under certain circumstances. I understand that all equipment, hardware, software, messages, information and files are the exclusive property of the Village. I agree not to use the electronic communications in a way that is disruptive, offensive, or harmful to others or to the Village. I agree not to use pass codes, access a file or retrieve any stored communication other than where authorized. I agree not to copy, send or receive confidential information without prior authorization from my immediate supervisor and the Village Administrator.

I am aware that the Village reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the Village's electronic communications systems at any time. I am aware that the Village may exercise these rights with or without employee notice, and that such access may occur during or after working hours. I am aware that use of a log-in name and password do not guarantee confidentiality, guarantee privacy or restrict the Village's right to access electronic communications. I am aware that violations of this policy may subject me to disciplinary action, up to and including discharge from employment, as well as civil and/or criminal liability.

I acknowledge that I have read and that I understand the Village's Information Technology policies, and have been afforded an opportunity to ask questions regarding the policies. I also acknowledge that I have read and that I understand this notice.

_____ _____

Signature of Employee Date

_____ _____

Signature of Supervisor Date

Copy for Employee
Copy for Employee's Personnel File