Village of Ashville
P.O. Box 195
200 East Station Street
Ashville, OH 43103
Office: 740/983-6367 ● Fax: 740/983-4703

POLICY AND PROCEDURE STATEMENT

SUBJECT	PAGE 1 OF 5	DATE EFFECTIVE
INTERNET & COMPUTER USE		APRIL 1, 2019
SECTION/POLICY NO. 5.16	APPROVED BY MAYOR VILLAGE ADMINISTRATOR PERSONNEL/BENEFITS COMMITTEE	SUPERSEDES VOA-O, AUGUST 31, 2009
PREPARED BY VILLAGE ADMINISTRATOR & PERSONNEL DIRECTOR		APPROVAL DATE 3/21/2019 / ISSUE DATE 4/1/2019 / REVIEW DATE
REFERENCE	REVIEW APPROVED BY PERSONNEL DIRECTOR	DISTRIBUTION LIST WEBSITE, MAYOR, COUNCIL, CLERK-TREASURER, AND VILLAGE EMPLOYEES

SCOPE

I. This Policy applies to Ashville Personnel, Ashville Government, and Contract Staff.

POLICY:

I. This Employee Internet Use policy is designed to help employees understand the Village of Ashville's expectations for granting employees access to the Internet and to help employees to use Village resources wisely. While a direct connection to the Internet offers a variety of benefits to the Village of Ashville, it can also expose the Village to some significant risks to its data and systems if appropriate security measures are not employed. Excessive, unnecessary Internet usage causes network and server congestion. It slows down other users, takes time away from work, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may expose the Village of Ashville and/or the individual user to significant legal liabilities.

PURPOSE:

I. To determine staff that needs to access the internet.

II. To provide standardized policy to appropriately access the internet.

III. To communicate to employee what is appropriate use of the internet.

IV. To have a standardized legal process.

PROCEDURE:

1. DEFINITIONS

- Domain Name - A domain name is the way to identify and locate an address on the Internet. The domain name is used to send e-mail, make FTP requests, etc. Before any message is sent on the Internet, the domain name is converted internally to a numerical address, an Internet protocol address, which is what computers on the Internet deal with directly.
- Electronic Mail - Electronic Mail (e-mail) may include non-interactive communication of text, data, images or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "e-mail,"" "facsimile," or "messaging" system; or voice messages transmitted and stored for later retrieval from a computer system.

- FTP - file transfer protocol; a program that allows you to transfer data between different computers on a network.
- Guidelines - Recommendations derived from experience and which should be used.
- Hacking - An unauthorized attempt or entry into any other computer. Never make an unauthorized attempt to enter any computer. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.
- Internet – The Internet is a network of connected sites accessible through a "web browser" and is a resource for research, information gathering, extending and obtaining services, and education through a common communications language, or "protocol".
- Internet Access – Internet access includes all available routes to the Internet, including direct Internet Provider access and Modem/ISP individual accounts.
- Mailing List - A service that sends e-mail to everyone on a list whenever e-mail is sent to the service, permitting a group of users to exchange e-mail on a particular topic.
- Netiquette - A combination of "network" and "etiquette." It is the practice of good manners in a networked environment.
- News Groups - Discussion groups with common themes on USENET.
- TELNET - A program that allows remote login to another computer.
- TCP/IP - Transmission Control Protocol/Internet Protocol; the communication protocol used by computers connected to the Internet.
- Trojan Horse – A destructive program that masquerades as a benign application. Unlike viruses, Trojan Horses do not replicate themselves but they can be as destructive.
- USENET - A collection of computer discussion (news) groups.
- Users - The public and Agency employees.
- Worm – A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as monopolizing the computer or network's resources and shutting systems down.
- Vendors: Any private person or business enterprise.
- Virus – A program or piece of code that is loaded onto a computer without the user's knowledge and runs against the user's wishes. It may contain a self-replicating component to spread the "infection."

Employee General Internet Usage Guidelines

1. The internet is a tool for meeting the official business needs of the Village. Internet access is considered Village property and the Village has the right to monitor the use of such property at any time. Therefore, users should not have any expectation of privacy as to their Internet usage via Village computers and networks.
2. Authorization for Internet access must be obtained through your immediate supervisor. Once authorization is approved you are responsible for the security of your account password and you will be held responsible for all use or misuse of your account. You must maintain secure passwords and never use an account assigned to another user.
3. The primary purpose of Internet use is to conduct official business. Employees may occasionally use the Internet for individual, nonpolitical purposes on their personal time, if such use does not violate the terms and conditions of this policy or interfere with Village business.
4. Users may not download, store, transmit, or display any kind of image or document on any department system that violates federal, state, or local laws and regulations, Executive Orders, or department adopted policies, procedures, standards, or guidelines.
5. E-mail requires extensive network capacity. Sending unnecessary e-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical Village business. When the Village grants an individual employee access to

the network, it is the responsibility of the employee to be cognizant and respectful of network resources.

6. Users may not attempt to access prohibited content or to circumvent software put in place by the agency to prevent such access.
7. If a user accidentally connects to a site that contains sexually explicit or otherwise offensive material, he/she must disconnect from that site immediately and report the incident to their supervisor.
8. Use of the Internet as described below is strictly prohibited:
    a. Viewing or distributing obscene, pornographic, profane, or sexually oriented material;
    b. Violating laws, rules and regulations by sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited.
    c. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.
    d. Never copy or transfer electronic files without permission.
    e. Encouraging the use of controlled substances for criminal or illegal purposes;
    f. Engaging in any activities for personal gain;
    g. Chain letters are illegal and may not be transmitted through e-mail
    h. Obtaining or distributing copyrighted information without permission;
    i. Never send, post or provide access to any confidential Village materials or information.
    j. Obtaining and distributing advertisements for commercial enterprises, including but not limited to, goods, services, or property;
    k. Violating or infringing upon the rights of others;
    l. Conducting business unauthorized by the department;
    m. Obtaining or distributing incendiary statements, which might incite violence or describe or promote the use of weapons;
    n. Obtaining or exchanging proprietary information, trade secrets, or any other privileged, confidential, or sensitive information that is not authorized;
    o. Engaging in any political activity prohibited by law; and
    p. Using the system for any illegal purpose.
9. Users may access any State owned web site for the purpose of conducting Village authorized business, such as the online payroll system, utility, ect, providing they have proper password or other security authorization.
10. Users may not knowingly or willfully create or propagate any virus, worm, Trojan Horse, or other destructive program code. Care must be done when downloading a file from the Internet. It can bring viruses with it. Scan all downloaded files with Village standard virus prevention software.
11. Almost all data and software is subject to the Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to you. Software which requires purchase or reimbursement for its use, such as shareware, requires strict adherence to the terms and conditions specified by the owner unless written permission for unrestricted use has been obtained. When in doubt consult your supervisor or designee.
12. Users may not download or distribute pirated software or data from any source nor any inappropriate images.
13. Users may only download software with direct business use and must take all necessary actions to have such software properly licensed and registered as required. Downloaded software must be used only under the terms of its license.
14. The Village has the right to inspect any and all files stored in secured areas of the Village the networks, on computing devices owned or leased by the Village, or on any other storage medium provided by the Village for Village business (i.e. flash drives, floppy disks, tapes, and RW CDs) in order to monitor compliance with this policy.
15. Authorized individuals, as part of their job responsibilities, may investigate and monitor Internet "links" appearing on Village owned web sites to insure linkage to inappropriate or unauthorized web sites does not exist. Discovery of any such violation will result in the immediate deletion of the "link" and a report to the leadership staff for further action.
16. An Internet user can be held accountable for any breaches of policy, security, or confidentiality resulting

from their use of the Internet. Such violations of this policy may result in disciplinary action.

17. You are obligated to cooperate with any investigation regarding the use of your computer equipment and which your general manager has authorized.

Employee E-mail Internet Usage Guidelines

1. MAIL ON THE INTERNET IS NOT SECURE. Never include in an e-mail message anything that you want to keep private and confidential because e-mail is sent -- unencrypted and is easily read.
    a. This policy can be impacted through communication with the solicitor or legal counsel. In that case email use will be clearly be identified as Confidential using the email "tagging and sensitivity" protocols.
2. Management has the right to access all e-mail files created, received or stored on Agency systems and such files can be accessed without prior notification.
3. Be careful if you send anything but plain ASCII text as e-mail. Recipients may not have the ability to translate other documents, for example Word or Word Perfect documents.
4. Be careful when sending replies - make sure you are sending to a group when you want to send to a group, and to an individual when you want to send to an individual. It is best to address directly to a sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors.
5. Include a signature (an identifier that automatically appends to your e-mail message) that contains the method(s) by which others can contact you. (Usually your e-mail address, phone number, fax number, etc.)
6. For important items, let senders know you have received their e-mail, even if you cannot respond in depth immediately. They need to know their e-mail is not lost.
7. Watch punctuation and spelling. It can reflect on your professionalism. Use automatic checking programs if available.

Internet Mailing Lists and Usenet News Groups

The e-mail guidelines apply here as well.

1. Be sure to change your mailing address if your account changes. Do not simply forward your e-mail from your old account to your new one. This creates a burden on the Village's information systems. Be careful when using auto-reply features in e-mail when you belong to mailing lists. Auto-reply replies are often sent to the entire list indiscriminately and your reply may not be important to all on the list; e.g. most do not care that you are on vacation, and worse, your message may have been intended for only one recipient.
2. As a new member of a news group, monitor the messages for a while to understand the history and personality of the group. Jumping right into the discussion may make you look foolish if you lack background information.
3. Do not re-post any messages without permission. Even messages may have copyright protection.
4. Do not post personal messages to a mailing list or USENET news group.
5. If you survey the group, as a courtesy, post a summary of the results.
6. Be sure to properly acknowledge with quotations any material borrowed from others. Be careful of plagiarism.
7. Do not post any messages anonymously. The professional community views this practice as bad form. As a matter of policy the USENET community and system managers are asked to track down offenders.
8. Be careful when you re-post any requests. Some requests are fraudulent.
9. State the subject of your message clearly in the subject line. Common subject lines can help in record retention.
10. Before joining mailing lists and news groups give thought to how much time these activities require. Also, for Usenet, look at the news, announce, new-users group. It contains information to assist you.
11. Be sure to read the Frequently Asked Questions (FAQs) for your group(s).
12. Never send angry messages (flames). If you receive a "flame," do not over react. Remember that not everyone is as polite as you are.

FTP (File Transfer Protocol)

1. These guidelines cover use of FTP (or download) sites. **It is best for the Village IS Service to FTP.**
2. Downloaded files may contain viruses. Scan all downloaded files with the Village's standard virus prevention software.

3. Do not FTP during your site's prime hours due to network impact on other users.
4. Look locally before downloading a file from a geographically remote site. Your system manager can help you find the closest site.

5. Do not download on the off chance you will "need it someday.'' Conversely, do not search for "neat stuff" to FTP. If you discover that you do not need what you have downloaded, delete it. You can always get it again if you discover you need it later.
6. Observe any posted restrictions on the FTP server.
7. Login using your real user name and node address as your password on anonymous FTP servers.

Netiquette

1. These are Netiquette (see Glossary) guidelines:
    a. Be cognizant of system etiquette. The computer you use may have limits regarding disk space usage. E-mail takes up space; therefore, you should regularly delete and/or archive any messages you wish to save.
    b. Remember that the recipient is a person with feelings. Since they cannot see you, they may not know when you are joking. Be sure to include visual or verbal clues. Convention indicates the use of the smiley face. :) (Look sideways).
    c. DO NOT SEND MESSAGES ALL IN CAPITALS. It looks as if you are shouting. Use initial capitals or some other symbol for emphasis. For example: That IS what I meant. That *is* what I meant.
    d. Remember that some people have to pay for each byte of data they receive. Please keep messages to the point without appearing terse or rude.

I have read and reviewed the Internet Policies and Guidelines (Guide). By signing this form, I agree to abide by the Guidelines currently in place and I agree to review periodically any changes or modifications. I recognize that the law and associated policy regarding the use of Internet, electronic mail and the Village's information systems are continually evolving. Therefore, I understand that my regular review of policy is required.

My fellow employees, be aware that your employer may not turn its surveillance into on the job voyeurism.

Employees have prevailed in court when employers claimed drugs as a reason for videotaping them without their knowledge. In one case, no illegal drugs were found, used or sold. The only things found were employees changing clothes exposed to hidden cameras.

Print Name: _____

Signature: _____ Date:_____

These rules require strict adherence. Any infraction thereof could result in disciplinary action. Disciplinary actions range from verbal warnings to termination; the severity of the misbehavior governs the severity of the disciplinary action.