ENDWELL FIRE DISTRICT

INTERNET COMPUTER USE AND COMMUNICATIONS POLICY	
Number: 2024-23	**Adopted: January 10, 2024**

PHILOSOPHY:

All Personnel are acting as representatives of the Fire District ("District") when using any communication resources provided by the District or connected to it or when conducting business on behalf of the District for any audience. Users of District-provided resources are held to the same standards whether the information being accessed is business-related or personal.

POLICY:

Communications resources including, but are not limited to: traditional mail, personal computer, palm pilots, electronic mail, text messaging, Intranet and Internet, telephones, voice mail, fax machines, cellular phones, modems, pagers, and calling cards are intended primarily for business use. The District recognizes and permits occasional personal use of District communication resources, with the exception of a District-provided calling card, provided that such use does not interfere with work responsibilities or other business needs or violate the law or District policy. The District acknowledges that all forms of communication resources are integral to our businesses and can be helpful tools in maintaining a balance between work and personal life.

All individuals are acting as representatives of the District when using any communication resource provided by the District or connected to it or when conducting business on behalf of the District for any audience. Users of District-provided resources are held to the same standards whether the information being accessed is business-related or personal.

Using electronic mail, text messaging, the Intranet, and the Internet :

Users of e-mail systems must make sure that incoming and outgoing e-mail documents and attachments are not infected with viruses. Information on the virus protection program can be obtained from the District Office.

The District recognizes that employees may need to maintain limited non-work-related files on their workplace computers. Non-work-related files should not be stored on a file server (shared network drive). Non-work-related files, to the extent they are permissible under this policy, should be stored on your PC's local hard drive (c: drive).

The District Network may be used only for lawful purposes. Without limitation of the foregoing, it is strictly prohibited to create, transmit, distribute, or store any information, data, or material which:

- Encourage conduct that would constitute a criminal offense or give rise to civil liability.
- Infringes any copyright, trademark, trade secret, or other intellectual property rights.
- Is obscene or constitutes child pornography.
- Is libelous, defamatory, hateful, or constitutes an illegal threat or abuse.

- Violates export control laws or regulations.
- Constitutes any form of gambling, chain letters, or threats.
- Creates a hostile work environment or is disrespectful or is in any way inappropriate.

District policy also strictly prohibits all of the following:

- Messages that are determined by the District to be defamatory, abusive, obscene, sexually oriented, threatening, harassing, or otherwise inappropriate.
- Messages that are determined by the District to be offensive or harassing in light of the District's Equal Employment Opportunity policy, Workplace Standards, Harassment and Discrimination, and Sexual Harassment policies.
- Messages that disclose confidential information about District operations, employees' services, or systems to any recipient not authorized to receive such information.
- Messages that involve conducting business on behalf of an entity other than the District or on behalf of any individual, including yourself.
- Messages that contain large attachments that are not business-related.
- An attempt by one employee to gain access to another employee's e-mail messages without that employee's express permission or District authorization.
- Attempts to break into any computer or exceed authorization privileges (cracking or hacking), whether at the District or another organization.
- Attempts to circumvent the authorization procedure or security of the following, but not limited to any host, network, network component, or account, to access data, accounts, or servers which the user is not expressly permitted or authorized to access. This prohibition applies whether or not the attempted intrusion is successful and includes unauthorized probes or scans performed with the intent to gather information on possible security weaknesses or exploitable configurations.

In addition, the District reserves the right to filter personnel access to specific Internet sites that are deemed as not business-related and/or inappropriate. Personnel who have a business need to access restricted sites must obtain management approval.

Violations of system or network security are prohibited and may result in criminal and civil liability. The District will investigate potential security violations and may notify applicable law enforcement agencies if violations are suspected/

Personnel who use communication resources improperly, and/or whose use results in injuring the reputation or image of the District or any District/Department personnel, or whose use impairs any employee's ability to meet the expectations and responsibilities of his or her job will be subject to disciplinary action up to and including termination of employment.

Communicating proprietary and confidential information:

Personnel must exercise caution when communicating proprietary and confidential information. Any communications of this type must be on a business need-to-know basis and such messages must be marked confidential. Personnel must not forward copies of proprietary or confidential information to inappropriate recipients inside or outside of the District. The transmission of confidential information through the Internet is prohibited unless consistent with District approved safeguards (encryption or other secure means) for transmitting such information.

Monitoring of Communication Resources:

The computers and computer accounts given to users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system or any other communication resources. Passwords for computer, electronic, and telephonic communication systems do not guarantee privacy and may be overridden by the District. The content of all internal and external communications utilizing District resources is the property of the District.

The District has the right to monitor and review the usage and content of any communication activity consistent with the law to determine whether there has been a breach of security or a violation of any District policy. In addition, the District maintains the right to access, audit, disclose, delete, and copy all communication resources usage and non-business-related content, for any legitimate business purpose. Keystroke entries may be monitored regardless of whether documents are saved or deleted. Anyone using District systems expressly consents to such monitoring.

Who is included under this policy:

All personnel are included in this policy. The Board of Fire Commissioners is responsible for ensuring that all contractors and temporary seasonal staff are held accountable for this policy. For the purpose of this policy, the term "Personnel" refers to all members and officers of the Fire Department and Fire Company and all employees, officers, and agents of the Fire District.

Roles:

Employee: Educates oneself and configures his or her systems with at least basic security as defined by the District. Immediately report any receipt or misuse of communication resources to the Chief's Office or District. Understands that the District monitors the use of communication resources. Does not disclose passwords or other log-on identification information to any party. Does not lend or share any equipment for which he or she is accountable (e.g., calling cards, pager, etc.).

Chief Officers: Reinforce this policy to employees regularly. Review the policy with employees if misuse of communication resources in the District or Department is suspected. Communicates this policy to new employees joining the District and/ or Department. Informs employees that usage of resources such as telephone, e-mail, text, Intranet, Internet, calling card, fax, and pagers

will be monitored and that Downloaded information is accessible and subject to review. Immediately notifies the District of any reports of misuse of resources to determine appropriate action.

Board of Fire Commissioners: Conducts review of evidence on usage of communication resources. Works with the District Counsel, if necessary. Assists employees and managers in addressing any issues or concerns.

Definitions:

Calling Card: Resource provided to allow for calling use on telephones outside the District when conducting District business.

Electronic Mail: Refers to electronic messages exchanged among District employees, customers, vendors, via the District's electronic mail network, etc.

Fax: Electronic equipment used in receiving and transmitting information over telephone lines.

Internet: Worldwide network of interconnected computer networks (that use Transmission Control Protocol/Internet (TCP/IP). Includes electronic mail (e-mail) and the Intranet.

Intranet: Internal information resource such as web pages that use TCP/IP accessible to specific populations.

Occasional Use: Use that does not have a negative impact on the District's resources as it relates to cost, time, and conflict of interest. Examples of occasional use are calling home to check on a child, making an infrequent copy on a Company copy machine, or faxing a document for closing on a home. Occasional use does not include ongoing, frequent, or repetitive applications (e.g., publishing team sports results).

Pager: Device used to notify a party that contact is requested.

Confidential and Proprietary Information: This applies to very sensitive internal information, which, if modified or disclosed, would have a legal, regulatory, financial, or negative public perception impact. Disclosure or modification could also adversely impact employees or the community.

Examples of confidential information include trade secrets, strategic plans, encryption keys and passwords, personal identification numbers (PINs), encryption documents, computer programs, customer information, customer lists, account information, employee salary, personnel information, and medical records.

Telephone: Any District-provided phone system. Also includes any use of phone the system that ultimately results in reimbursement by the District. Includes telephone bills as well as equipment.

Text Messaging: The sending of text messages by use of a cellular phone or other device provided by the District.

Traditional Mail: Any source of paper mail, either internal or external.

QUESTIONS?

If employees have questions about this policy or other policies or need to speak to someone for further information, they should contact the Chief's Office or the Board of Fire Commissioners.

FREQUENTLY ASKED QUESTIONS:

1. What are some examples of acceptable occasional personal usage?
2. Are there any circumstances when a Corporate Calling Card can be used for personal calls?
3. What is considered inappropriate usage of Communication Resources?
4. Who determines if an employee should have access to certain Internet sites that are currently restricted by the District?

Q: What are some examples of acceptable occasional personal usage?

A: Examples of occasional personal usage are:

- Calling, e-mailing, and paging home to check on a child;
- Using the Internet to book your annual vacations, place an order, review stock performance;
- Making an infrequent copy of a personal document, and
- Paying bills over the phone or via the Internet.

Occasional use does not include ongoing, frequent, or repetitive applications (e.g., publishing team sports results). If an employee spends excessive amounts of District time or resources managing personal matters, he/she may lose further access to these resources, and disciplinary action may be taken, up to and including termination. A volunteer's personal time will be treated differently than personal time spent on computers by a paid employee.

Q: Are there any circumstances when a Corporate Calling Card can be used for personal calls?

A: A Corporate Calling Card is issued strictly for business purposes. However, according to the Travel Policy, employees traveling on business trips of one night or more are authorized to use the Corporate Calling Card to place one call home per day. For more details, please see the Travel Policy.

Q: What is considered inappropriate usage of Communication Resources?

A: There is no all-inclusive list of behaviors considered inappropriate when using communication resources. Some examples of inappropriate usage include:

- Use of voice mail, calling card, pager, fax, and telephone by someone other than the party to whom the device or resource was issued;
- Accessing inappropriate resources and/or materials (e.g., 900#s, sexually explicit magazines, hate materials);

- Sending threatening messages;
- Sending chain letters;
- Sending racially and/or sexually harassing or offensive messages;
- Sending messages that violate District policy and
- Sending messages that could damage the image or reputation of the Department or District.

Q: Who determines if an employee should have access to certain Internet sites that are currently restricted by the District?

A: It is the Board of Fire Commissioner's responsibility to determine if an employee should be exempt from the current policy. An exemption will require the employee to access the Internet via a modem to bypass the proxy server and filtering software. To address security concerns related to modems, the employee will be restricted to using a PC that is not connected to the District network. In addition, security software will be utilized to control logins to the PC.

The adoption of the foregoing policy in the form of a resolution was duly put to a vote, and upon roll call, the vote was as follows:

Chairman	Carlton "Andy" Anderson	AYE
Commissioner	Donald "Don" Battaglini	NOT PRESENT
Commissioner	Mark Storm	AYE
Commissioner	Michael Hamzik	AYE
Commissioner	Michael Lewis	AYE

The resolution was thereupon duly adopted.

Dated: Endwell, New York
January 04, 2023

This policy was reviewed and re-adopted on January 10, 2024, and supersedes any previous reversion of this policy.

By order of the Board of Fire Commissioners, Endwell Fire District.

Reviewed and Adopted: January 10, 2024
Rescinds Policy: 2021-09
COMPUTER / INTERNET USAGE
Reviewed and Adopted: July 21, 2021
Adopted by the Board of Fire Commissioners
February 20, 2014