CLARENCE FIRE DISTRICT NO. 1

Computer/Acceptable Use Policy

I. Scope

This policy applies to all individuals with access to technology provided by the Clarence Fire District # 1.

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Clarence Fire District #1 business or interact with internal networks and business systems, whether owned or leased by Clarence Fire District #1, the user, or a third party. All users, contractors, consultants, temporary, and other workers at Clarence Fire District #1 are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Clarence Fire District #1 policies and standards, and local laws and regulation.

This policy applies to users, contractors, consultants, temporaries, and other workers at Clarence Fire District #1, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Clarence Fire District #1.

II. Definition

For the purpose of this document an [USER(S)] is defined as someone who is authorized and commissioned to act on behalf of Clarence Fire District #1.

III. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Clarence Fire District #1. These rules are in place to protect the user and Clarence Fire District #1. Inappropriate use exposes Clarence Fire District #1 to risks including virus attacks, compromise of network.

IV. Policy

IV.1 General Use and Ownership

IV.1.1 Clarence Fire District #1 proprietary information stored on electronic and computing devices whether owned or leased by Clarence Fire District #1, the user or a third party, remains the sole property of Clarence Fire District #1. Users must ensure through legal or technical means that proprietary information is protected.

IV.1.2 Users have a responsibility to promptly report the theft, damage, loss or unauthorized disclosure of Clarence Fire District #1 proprietary information.

IV.1.3 Users may access, use or share Clarence Fire District #1 proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

IV.1.4 Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, users should consult the Clarence Fire District #1 IT Department.

IV.1.5 For security and network maintenance purposes, authorized individuals within Clarence Fire District #1 may monitor equipment, systems and network traffic at any time.

IV.1.6 Clarence Fire District #1 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

IV.1.7 Clarence Fire District #1 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

IV.1.8 Information and data stored on individual PCs is not backed up. As a result, critical documents and spreadsheets must not be stored on individual PC hard drives. (Note: There may be some instances in which storing information locally is required by a software package. Special procedures will be taken in these cases.) Each user has a special, secure area on the network file server, designated as their (U:) drive or Users directory, where all information not needed by others should be stored. Shared information, which others may need to access, must be stored under shared areas of the network, such as the (F:) data drive on the network file server.

IV.1.9 Users are required to maintain their computers and related equipment in good working order. If any of your equipment needs services, repair or maintenance, notify the district IT Department by submitting a "computer system problem form" (see Attachment 1) to the Fire District Secretary.

IV.2 Security and Proprietary Information

IV.2.1 All external mobile and computing devices that connect to the internal network or wireless network must be approved by Clarence Fire District #1 IT department**.**

IV.2.2 System level and user level passwords must comply with the network password policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

IV.2.3 All computing devices must be secured. Users must lock the screen or log off when the device is unattended.

IV.2.4 Postings by users from a Clarence Fire District #1 email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Clarence Fire District #1 unless posting is in the course of business duties.

IV.2.5 Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware or viruses.

IV.3 Unacceptable Usage

The following activities are, in general, prohibited. Users may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access if disrupting production services).

Under no circumstances is a user of Clarence Fire District #1 authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Clarence Fire District #1 owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

IV.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Clarence Fire District #1.

2. Accessing data, a server or an account for any purpose other than conducting Clarence Fire District #1 business, even if you have authorized access, is prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members.

6. Using a Clarence Fire District #1 computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any Clarence Fire District #1 account.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

9. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec and the Clarence Fire District #1 IT Department is made.

10. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.

11. Circumventing user authentication or security of any host, network or account.

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

13. Providing information about, or lists of, Clarence Fire District #1 users to parties outside Clarence Fire District #1.

V. Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the Clarence Fire District #1. Whenever users state an affiliation to Clarence Fire District #1, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Clarence Fire District #1 ". Questions may be addressed to the IT Department.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5. Use of unsolicited email originating from within Clarence Fire District #1's networks of other Internet service providers on behalf of, or to advertise, any service hosted by Clarence Fire District #1 or connected via Clarence Fire District #1's network.

6. District provided email is for firematic purposes only. Personal use should be kept to an absolute minimum.

7. All emails, sent or received, are District records and as such, are accessible to appropriate staff members. Any e-mail sent or received is subject to current FOIL (Freedom of Information Law) guidelines, set forth by New York State.

8. No anonymous emails can be sent from District systems. All users are required to identify themselves by name and email address.

9. Chat room participation is prohibited except for firematic business related forums which require prior approval from the Commissioner in charge of technology.

VI. Policy Compliance

VI.1 Compliance Measurement

The Clarence Fire District #1 IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

VI.2 Exceptions

Any exception to the policy must be approved by the Clarence Fire District IT team in advance.

VI.3 Non-Compliance

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination.

This policy is adopted on October 20, 2020 and rescinds any previous version of this policy.
By order of the Board of Fire Commissioners, Clarence Fire District No. 1.

Attachment 1

CLARENCE FIRE DISTRICT NO. 1
COMPUTER SYSTEM PROBLEM FORM

Date of Problem: _____

Computer Terminal Location: (please check one)

_____ Chief's Office _____ Chief's Laptop

_____ Copier Room _____ District Office

_____ Rescue 5 laptop _____ Equipment Room

_____ President's Office

Description of Problem (please include as much detail as possible):

_____

_____

_____

_____

_____

Problem reported by: _____

Phone numbers to reach you for additional questions: _____

****

	Dates	Signatures
Logged by District Secretary:	_____	_____
Copied to Commissioner:	_____	_____
Problem corrected:	_____	_____
Form returned to originator:	_____	_____

Instructions:

1.) Original form shall be submitted to Fire District Secretary.
2.) When resolved, copy shall be returned to District Secretary to document dates.
3.) A copy of the completed form shall be returned to the originator by the District Secretary. The original form will be kept on file in the District Office for future reference.