North Kingstown Fire Department

Standard Operating Guidelines		2000 Series
Effective Date:	Computer Usage	Human Resources
04/2021		2113
Revision Date:		
04/2021		Page 1 of 3

I. PURPOSE

To establish guidelines for the appropriate use of the North Kingstown Fire Department's (Department) computer network and storage system.

I. BACKGROUND

As a policy, the Department encourages personnel to use station computers for departmental work, as well as individual training needs, outside career development courses, and other special projects related to the Department.

II. POLICY

The Town of North Kingstown (Town) in conjunction with the Department permit access and use of electronic communication systems to input or retrieve job-related information as needed to meet job-related requirements.

The following activities are prohibited while using Department (Town) electronic resources:

A. Creating, accessing, inputting, copying, transmitting, or forwarding information in any form, which contains obscene, indecent, lewd, abusive, or threatening material or which constitutes illegal activity.
B. Creating, accessing, inputting, copying, transmitting, or forwarding information in any form, which is offensive, intimidating, harassing, disparaging, hostile, or profane on the basis of race, color, gender, religion, national origin, disability, age, veteran status, or any other legally protected status.
C. Engaging in any activity that would compromise the security of any Department and/or Town's information system.
D. Unauthorized copying, reproducing, or disseminating copyrighted or licensed materials (including printed material or software). This does not include departmental policies, procedures, guidelines, general orders, and rules and regulations. These materials may be shared with the permission of the Fire Chief and/or designee.
E. Communicating any information concerning any password identifying code, personal identification number, or other confidential information without the permission of the Fire Chief, Town Manager, or the Town's IT personnel.
F. Creating, modifying, executing, or re-transmitting any computer program or instruction intended to gain unauthorized use/access to the Town's and/or other computer system or software.

G. Creating, modifying, executing, or re-transmitting any computer program or transmission intended to obscure or hide the identity of the sender or electronic messages and/or alteration of system and/or user data used to identify the sender.
H. Accessing or intentionally destroying software in a Department (Town) electronic communication system without the specific instruction and permission of a system administrator.
I. Violating any law or participating in the commission or furtherance of any crime or other unlawful or improper purpose using Department (Town) electronic communication system. This includes copyright infringement.
J. Using the Department's (Town's) electronic communications system in a manner inconsistent with the Department's policy.
K. Engaging in commercial activities and/or secondary employment activities using the Department's (Town's) electronic communication systems including, but not limited to, offering service or merchandise for sale or personal gain.
L. Disclosing confidential information without the prior approval of the Fire Chief and/or designee.
M. Loading or installing new software without the prior approval from the Fire Chief and/or designee, and/or system administrator.

Company officers will be responsible for monitoring computer usage to ensure compliance by all personnel under their command.

The Department expects personnel to conduct themselves professionally while using Department resources (including electronic communications systems and email), and personnel shall refrain from using Department resources for activities disruptive to the workplace or in violation of the public trust.

Internet Usage

The Department's (Town's) electronic communication systems do not offer privacy protections. Authorized users (i.e. Department personnel) do not have any privacy right in any matter created, received, or sent via electronic communication systems. The Department reserves the right, without any advance notice, at any time, to monitor, access, or disclose any message created, received, or sent using the Department's (Town's) electronic communications system. Internet usage is monitored and recorded. The Fire Chief and/or designee and/or system administrator may access any user's electronic communication files if monitoring reveals possible evidence of criminal activity or misconduct. Departmental and/or Town officials may provide such evidence to law enforcement officials if deemed appropriate.

The Department (Town) encourages personnel to use the internet to support and accomplish the mission of the Department. Use of the internet requires responsible judgement, discretion, and compliance with

applicable laws and regulations. Users must be aware of security and privacy concerns. Users must follow directives concerning internet usage.

Outlook – Email

The Department encourages the use of station computers for electronic correspondence to Department members and other Town departments. Like other Town-related electronic information resources, Outlook is owned by the Town and is monitored. E-mails generated through the Department's electronic communications system are public record and subject to disclosure.

To ensure resources are not abused, the Department developed the following guidelines:

A. All department personnel shall be responsible for checking their email account at the beginning of their workday and/or work shift ***(See also, SOG# 2011 – Employee Web-Mail)***
B. All personnel will not forward or draft any e-mail containing illicit, vulgar, or otherwise socially unacceptable material. If such material is received from an outside source, it will be the responsibility of the individual receiving the e-mail to delete and not forward it.
C. All officers shall be responsible for ensuring the station account (Station Computer) is checked each day, prior to 0900 hours.
D. In the event that a member is "locked-out" or otherwise cannot access their email, they shall report this to their supervisor to resolve.

Department-wide Email distribution requires authorization from a member of the Department's command staff. In the event, an officer (non-command staff) or a firefighter wish to send a department-wide email, authorization must be received by a member of the command staff. The sender shall identify the Chief, Deputy Chief, Battalion Chief, etc. that authorized the department wide distribution within the email.