Town of Deerfield
Office of the Selectboard
&
Board of Health

Deerfield Municipal Offices
8 Conway Street
South Deerfield, MA 01373
Ph: 413-665-1400
Fax: 413-665-1411

Policy for Acceptable Use of Town Information Technology Systems and Personal Electronic Devices

I. PURPOSE AND SCOPE

The purpose of this Policy is to set forth rules governing the use of the Town's information technology infrastructure and telecommunications systems (collectively "IT systems"). This Policy ensures that the use of Town IT systems is consistent with other Town policies, applicable law, employee job duties, and the Town's business interests.

For the purposes of this Policy "IT systems" shall include, without limitation, Town-owned or Town- leased computers, laptops, tablets (such as iPads), hardware and software, electronic mail ("e-mail"), electronic files, telephones, cellular phones, pagers, "blackberry"-style devices, smartphones, facsimile machines, official Town social media accounts, and the Internet.

This Policy applies to all Town employees; however, to the extent that this Policy conflicts with the provision(s) of an employee's collective bargaining agreement, such agreement will control.

The use of Town IT systems by any employee, contractor, consultant or other user ("users") shall constitute acceptance of the terms of this Policy and all other applicable Town policies.

II. APPLICABLE LAW AND OTHER TOWN POLICIES

Use of Town IT systems are subject to all applicable state, federal, and local laws and Town policies, specifically those that govern intellectual property protection, employment discrimination, misuse of Town resources, privacy rights, and confidentiality.

III. EXPECTATION OF PRIVACY

The Town provides IT systems to employees for business purposes. All such IT systems and all data, software, or other content transmitted by, received from, or stored on the same are the property of the Town and may be accessed and retrieved by the Town at any time.

I addition, designated network administrators may monitor network traffic, and/or access all files, including, without limitation, e-mail files and Internet use history, stored on Town IT systems.

Town employees therefore have no reasonable expectation of privacy in any data transmitted, received, and stored on an/or through the Town's IT systems.

IV. USERNAMES AND PASSWORDS

All usernames and passwords are for the exclusive use of the individual to whom they are assigned ("owner"). The owner is personally responsible and accountable for all activities carried out under his/her username and should take all reasonable precautions to protect his/her password. Owners are prohibited from disclosing their username and/or password to any person other than the Town's Systems Administrator. Town employees are prohibited from using, or attempting to use, another owner's username and/or password.

V. USE OF TOWN IT SYSTEMS

When using the internet on any of the Town's Systems, Town employees must adhere to the following:

A. Using the Town Systems for anything other than Town business is strictly prohibited.

B. Users must notify the Town's Systems Administrator immediately if they have any reason to believe that one of the Town's Systems has been infected with a computer virus, spyware, worm, trojan horse, trap door, or other malware; or that someone has attempted to do so. In addition, users are prohibited from using any computer virus, worm, trojan horse, trap door, spyware, or other malware on Town IT systems.

C. Users shall not access or use Town Systems for which they have no authorization to do so.

D. Users are prohibited from disabling, defeating, or circumventing any Town IT system security measure or attempting to do the same.

E. Users are prohibited from intercepting communication intended for other persons.

F. Users are prohibited from downloading any software or electronic files one of the Town's System onto their personal computers, laptops, smartphones, or tablets unless they receive express written permission to do so by the Town's Systems Administrator.

G. Users are prohibited from installing, updating, or upgrading software on the Town's Systems unless they receive express written permission to do so by the Town's Systems Administrator.

H. Users are prohibited from disclosing confidential or proprietary Town information unless they receive express written permission to do so from their department head or immediate supervisor;

I. Users are prohibited from engaging in any unlawful discrimination or any other unlawful activity on Town Systems.

J. The use or storage of any image, video, or document that is obscene, pornographic, sexually explicit or sexually suggestive on Town IT systems is prohibited, unless doing so is necessary to conduct official Town business, such as, by way of example and not limitation, workplace investigations and investigations of citizen complaints.

VI. USE OF TOWN EMAIL

The Secretary of State's Office of the Commonwealth has determined that email qualifies as "public records," as defined in G.L. c. 4, § 7 cl. 26th. Therefore, all email sent by or received through Town Systems shall be archived by the Systems Administrator. All users shall retain either a printed or digital record of e-mail sent by or received through the Town Systems in the same manner that other paper records are kept by their departments, and in accordance with the Record Retention requirements.

Users should be aware that opening programs or files attached to email messages may cause computer viruses to infect Town Systems, and thus should only open such attachments from anticipated and trusted sources.

Town Employees are prohibited from sending a single email to all Town employees unless expressly permitted to do so by the Town Administrator.

VII. USE OF TOWN CELLULAR TELEPHONES

Like emails, text or other messages sent via Town cellular phones, Smartphones, and blackberry-style devices may constitute public records, and therefore, any such messages pertaining to official business of the Town should be maintained as public records, in the same manner as email messages (see Section VI above).

VIII. USE OF PERSONAL ELECTRONIC DEVICES

For the purposes of this Section "personal electronic devices" shall mean computers, laptops, tablets (such as "iPads"), cellular phones, smartphones, "blackberry"-style devices, and devices with similar abilities that are worn like a wristwatch (such as an Apple Watch or Fitbit).

Employees are permitted to use personal electronic devices while on duty, provided that such use:

A. Is of little or no cost to the Town;

B. Is brief and infrequent;

C. Does not interfere with the user's job duties;

D. Does no disrupt the job duties of Town employees;

E. Dose not disrupt Town business;

F. Is consistent with all applicable Town policies and Federal, State, and local law; and

G. Is not used to access, download data or other content from, or upload data or other content to any Town IT system, unless permitted to do so under Section V above.

Any other use of personal electronic devices while on duty is prohibited.

IX. VIOLATIONS

Violation of this Policy may result in either the suspension or permanent loss of the privilege to use Town Systems. It may also result in discipline, up to and including termination from employment. In addition, users shall be personally liable for any losses, costs, or damages incurred by the Town related to violations of this Policy.

Illegal use of Town Systems may result in referral to municipal, State, and/or Federal law enforcement authorities.

Employees shall report violations of this Policy to their Supervisor, or in the case of Department Heads, directly to the Town Administrator. Any form of retaliation against another user for reporting a violation of this Policy is strictly prohibited.