TOWN OF SANDWICH

INFORMATION TECHNOLOGY RESOURCES USE POLICY

(Policy Attachment #6)

JULY 21, 2022

Adopted:
Updated April 20, 2021
October 25, 2018
June 25, 2018
July 26, 2012
May 3, 2007
August 23, 2001

TOWN OF SANDWICH

Information Technology Resources Policy

TABLE OF CONTENTS

INFORMATION TECHNOLOGY RESOURCES (ITR) POLICY

1.0 Purpose

This document describes the formal policy for employees and users of all Town of Sandwich ("the Town") Information Technology Resources (ITRs) including telephones, cell phones, computer hardware, software and peripherals, networks, printers, e-mail, the Internet and/or other electronic communication devices or technologies. Use of Town ITRs by any employee or user shall constitute acceptance of the terms of this policy and any such additional policies.

The purpose of this policy is to clearly define the policies of the Town and to direct the responsible and appropriate use of ITRs. This policy will be strongly enforced and employees and users of the Town's ITRs shall follow this policy at all times. Failure to comply with the provisions of this policy shall be grounds for disciplinary action and/or termination or suspension of use privileges. This document will be routinely updated and employees will be notified of any changes made.

2.0 User Responsibility

It is the responsibility of all persons using Town ITRs to read, understand and follow this policy. Questions or requests for clarification shall be submitted in writing to the Assistant Town Manager. All employees will be required to sign a statement acknowledging that they have read and understand this policy. The original will be kept on file at the Human Resources Department. A copy will also be filed in the employee's personnel file. In addition, employees are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of ITRs in accordance with Section 25.0 of the Town's Personnel Policies and Procedures.

3.0 Acceptable and Unacceptable Uses

The Town believes that ITRs used appropriately to support the employee's job duties and responsibilities empower users to deliver better services at lower costs. As such, employees are encouraged to use ITRs to the fullest extent in pursuit of their departmental goals and objectives. All ITRs are to be used in an appropriate, responsible, efficient, ethical, and legal manner. Access to ITRs is to be considered a privilege which can be suspended and/or terminated by the Town.

4.0 Data Confidentiality

In the course of performing the duties and responsibilities of their job Town employees and users have access to confidential and/or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or users to

acquire access to confidential data unless such access is required as a function of their job. Under no circumstances may employees or users disseminate any confidential information to which they have rightful access unless such dissemination is required as a function of their job.

5.0 Copyright Protection

Employees and users of Town ITRs must respect the rights of intellectual property owners.

6.0 Network Security

Users should avoid compromising the security of the network by protecting passwords and by "logging off" the network when leaving a personal computer unattended for extended periods of time.

7.0 ITR Use

Internet service is available to Town staff as an information resource upon approval of the employee's supervisor. The Internet is to be used to support the employee's job duties and responsibilities. It is a shared resource to be used where a clear benefit to the Town exists. Internet use is a revocable privilege and should be used in compliance with this policy. In addition, electronic mail ("e-mail") can provide excellent means of communicating with other employees, outside vendors and colleagues, and other businesses. Use of the Internet and e-mail, however, must be tempered with common sense and good judgment.

Use of the Internet and e-mail is a privilege, not a right. If you abuse these privileges, you will lose them. In addition, you may be subject to disciplinary action, including possible termination from employment, and civil and criminal liability.

7.1 Disclaimer of liability for use of Internet.

The Town is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk.

7.2 Duty of care.

Employees should endeavor to make each electronic communication truthful and accurate. You should use the same care in drafting e-mail and other electronic documents as you would for any other written communication. Please keep in mind that anything created or stored on the computer system may, and likely will, be reviewed by others.

Employees and users of e-mail must follow certain protocols. Because e-mail addresses identify the organization that sends the message, users should consider e-mail messages to be the equivalent of letters sent on official letterhead, and should ensure that all e-mails are written in a professional and courteous tone. Although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. Therefore, users shall not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

7.3 Duty not to waste computer resources.

Employees must not perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to: sending or forwarding mass mailings or chain letters to any e-mail address; spending excessive amounts of time on the Internet; playing games; engaging in online chat groups; social media for personal (non-work related) use; printing multiple copies of documents; or otherwise creating unnecessary network traffic.

Because audio, video, and picture files require significant storage space, files of this sort may not be downloaded unless they are business or job-related. This includes accessing Internet based radio or TV stations that offer streamed broadcasts. These types of websites maintain constant connections and continuously send data across the town's network, which slows down everyone else's Internet access. Personal photos may be brought in from home and used to customize your PC desktop environment on your Town-assigned personal computer or notebook provided that the content comply with Section 7.9 of this Policy. The Town will not be responsible for any personal files that reside on your Town-assigned computer. All employees are reminded that all ITR's are the property of the Town of Sandwich and as such everything is public.

E-mail attachments represent an impact on network capacity and shall only be used to communicate official business documents to recipients. The forwarding of any non-business related information is in violation of this policy. Employees who are the recipients of non-business related e-mail with or without attachments shall delete them immediately and shall under no circumstances forward them to anyone. E-mail attachments that are received from an unknown party should be considered "suspicious" and shall not be opened until the senders' identity can be confirmed. Many viruses are spread using e-mail systems in this manner.

7.4 No expectation of privacy.

The computers and computer accounts given to employees are intended to assist them in performance of their jobs. You do not and should not have an expectation of privacy in anything you create, store, send, or receive on the computer system. The computer system belongs to Town and may only be used for business purposes.

7.5 No privacy in communications.

Employees should never consider electronic communications to be either private or secure. E-mail may be stored indefinitely on any number of computers, including that of the recipient. Copies of your messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect usernames may be delivered to persons that you never intended.

7.6 Public documents.

The Town is a public governmental agency. As such, any and all electronic communications sent or received on Town computers are considered public documents and are subject to disclosure under the Massachusetts Public Records law, M.G.L. c. 66, §10. It should be noted that even deleted messages might be subject to disclosure because they still exist on backup tapes.

7.7 Monitoring of computer usage.

The Town has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring and/or restricting access to websites visited by employees on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users.

7.8 Blocking of inappropriate content.

The Town will employ means to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by the Town's network. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to blocking measures and notify your supervisor immediately.

7.9 Prohibited activities.

Material that is fraudulent, harassing, embarrassing, discriminatory, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (bulletin board systems, newsgroups, chat groups), downloaded from the Internet, or displayed on or stored in Town computers and/or servers.

7.10 Employer's computers.

Employees encountering or receiving the type of prohibited materials referenced above should immediately report the incident to the Assistant Town Manager and the I.T. Director.

7.11 Games and entertainment software.

Employees may not use the Town's Internet connection to download games or other entertainment software, including screen savers, or to play games over the Internet or use social media for non-work related purposes.

7.12 Accessing the Internet.

To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to the Town's network must do so through an approved Internet firewall. Accessing the Internet directly, by modem or other wireless methods, is strictly prohibited unless the computer you are using is not connected to the Town's network.

7.13 Virus detection.

All Town computers will be equipped with anti-virus software. Files obtained from sources outside the Town, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards or other online services, files attached to e-mail, and files provided by vendors or other third parties, may contain dangerous computer viruses that may damage the Town's computer network. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-system sources, without first scanning the material with approved virus checking software. If you suspect that a virus has been introduced into the network, immediately notify the Assistant Town Manager and the I.T. Director.

7.14 Altering attribution information.

Employees must not alter the "From" line or other attribution-of-origin information in e-mail, messages, or postings. Anonymous or pseudonymous electronic communications are forbidden. Employees must identify themselves honestly and accurately when making postings to newsgroups, sending e-mail, or otherwise communicating online.

7.15 Use of encryption software.

Employees may not install or use encryption software on any of the Town's computers without first obtaining written permission from the Information Technology Steering Committee through the Assistant Town Manager. You must not use passwords or encryption keys that are unknown to the Town.

7.16 Export restrictions.

The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States without prior written authorization from the Information Technology Steering Committee through the Assistant Town Manager.

8.0 Enforcement

All ITRs are the property of the Town of Sandwich and are to be used in conformance with this policy. The Town of Sandwich retains the right to, when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, exercise the authority to inspect any user's computer, and data contained in it, and data sent or received by that computer.

Users should be aware that the Town's network administrators, in order to ensure proper network operations, routinely monitor network traffic. Use of Town ITRs constitutes express consent for the Town to monitor and/or inspect any data that users create or receive and any messages they send or receive, and any web sites they access browsing the Internet. Reasons for monitoring may include, but are not limited to, review of employee productivity, investigations into claims of possible criminal activity and investigations into violations of this policy.

Failure to comply with this policy or other rules, regulations, state or federal laws may result in disciplinary action. If violations of this policy are discovered or suspected, the Town Administrator and/or Department Head shall act in accordance with the Town's Disciplinary Policy, Section 20.0 of the Personnel Policies and Procedures.

9.0 ITR Requests

Requests for new ITRs must be forwarded in writing to the Information Technology Steering Committee through the Assistant Town Manager. Requests will be handled on a priority basis, dependent on funding. Requests for hardware, software or peripherals different from the Town's standard configuration will only be authorized if the request can be justified as serving a business and public service need.

10.0 Software and Hardware Installation

Employees are not allowed to install personally owned hardware and/or software on a Town ITR. A request for hardware and/or software installation on a Town computer must be made first to the employee's supervisor who will forward the request on to the I.T. Director. The I.T. Director has the right to refuse installation.