TOWN OF NANTUCKET

Board of Selectmen

INTERNET, E-MAIL AND COMPUTER USE POLICY

Adopted: November 4, 1998
Effective: November 4, 1998
Updated: May 1, 2002; January 30, 2004; Dec 15, 2012; Aug 14, 2013

Applicability: *All Town and County employees*

I. Purpose

The safety and well being of each employee and citizen who comes in contact with the Town of Nantucket electronically, is of vital concern to the Town. Internet access and E-mail offer an easy, efficient and fast means of communication and/or research, but this use must be undertaken responsibly. The purpose of this policy is to:

- decrease the Town's liability exposure caused by an employee's inappropriate use of email or Internet access
- manage efficient use of computer systems; ensure that Town employees are using computers and Internet access appropriately and for Town-related purposes
- prevent unlawful or wrongful actions against employees or citizens either directly or indirectly through the use of computers
- prevent the possibility of endangering Town information systems by downloading files that contain viruses

II. Policy

Internet access, E-mail (both internal and external), and/or all other computer files and equipment provided by the Town of Nantucket are to be used for Town business purposes. In general, the use of computers or other Town equipment for personal purposes is prohibited. Employees will be allowed to access personal E-mail during the work day for a limited amount of time. This time will be controlled and monitored. An employee may, outside of working hours and for short periods of time, check one's personal email or access the Internet in a reasonable manner.

Access to the Town's network, computers, files, e-mail and the internet is controlled by assigned user accounts and passwords. Do not share Town of Nantucket passwords with anyone, except as requested by the Information Technology Department. All passwords are to be treated as sensitive, confidential Town information. Password protection or a "personal" computer does not imply that the user's messages, memos,

documents or any other files, active or deleted, are private.

Consistent with federal law, the Town reserves the right to enter, search, disclose, and monitor the computer files, E-mail and web access of any employee at any time and for any reason with or without advance notice. This includes, but is not limited to, investigating theft, disclosure of confidential information, personal abuse of the system, conflict of interest or monitoring workflow or productivity. Unauthorized computer users may not access the messages or files of other individuals on the Town's computer system. If an individual believes there is reason to access another employee's files and/or messages, that person should review his/her concern with their Department Head or the Town Administrator.

This policy is not only for the protection of the Town's employees, but also for the Town as a whole. Town PC's are connected to the Town's network and no risk can be tolerated.

III. Procedure for Internet Access and Use

1. Access to any inappropriate or offensive Internet site by any employee is prohibited. Examples of such Internet sites include: pornographic sites, sites that advocate illegal acts.

2. Access to the Internet shall be with the use of Internet Explorer as installed by the Information Technology Department. The Information Systems Administrator must approve any other software used to access the internet.

3. Access to the internet may be monitored on a regular basis to ensure that internet access is not being abused.

IV. Procedure for E-mail Access and Use

1. Access to Town of Nantucket E-mail accounts shall be through a Microsoft product (Outlook) as installed by the Information Technology Department or through Outlook Web Access.

2. Care should be taken to protect mobile devices that are configured to connect to the Town of Nantucket's e-mail system.

3. Any new E-mail accounts must be authorized by the appropriate Department Head through Town Administration and the Information Systems Administrator.

V. Procedure for Computer Access and Use

1. All software and computer equipment used by the Town must be approved and installed by the Information Technology Department.

2. Any new network accounts must be authorized by the appropriate Department Head through Town Administration and the Information Systems Administrator.

VI. Prohibited Computer, Internet and Email Activities

1. Attempting to gain unauthorized access to any computer system or network.

2. Deliberate attempt to disrupt the computer system performance or destroy data by spreading or introducing computer "viruses".

3. Use of the system to engage in any illegal act such as drug sales, lotteries, betting pools or criminal activities. Users shall not use the Internet or E-mail system to threaten another person's safety or to access material that is profane, obscene, advocates illegal acts of violence, or for any other inappropriate purposes. Users shall not forward any of the above for any reason. Contact the Information Systems Administrator for instructions on clearing any offensive email if necessary.

4. The use of Town information for non-Town purposes is prohibited. This expressly prohibits Town employees from accessing the system to provide information outside the realm of the employee's direct responsibilities and/or outside established procedures for responding to requests for public information.

5. Destruction of or damage to any equipment, software or data belonging to the Town of Nantucket.

6. Use of computer games during working hours is prohibited.

7. Use of inappropriate language (i.e., use of obscenities, profanity, threats, racist or sexist remarks), which applies to public messages, private messages and material posted on Web pages.

8. Knowingly or recklessly posting false or defamatory information about a person or organization.

9. Using the system for political lobbying, personal financial gain or fraud.

10. Establishing web sites unless directed by Town Administrator.

11. Accessing or downloading resources of any kind for which there is a fee; downloading information or files unless information has previously been scanned with virus detection software; downloading files that are too large (any files of this type should be sent to the Information Systems Administrator and will be transferred to your machine via the network) and will tie up or disrupt the system; downloading or accessing information resources which are not for a clear Town purpose.

12. Forwarding or saving "spam" or any other unauthorized unnecessary email or data on any Town computer unless requested to do so by the Information Technology Department.

13. Office wall ports look like phone jacks but they connect directly into the Town's network. Nothing should be plugged into these ports unless approved or authorized by IT. All equipment moves should be coordinated through the IT department.

14. Town-issued laptops are configured to communicate using a wireless adapter. They are not set up to connect directly into the Town's network. When using your Town-issued or personal laptop at work you should use the Town's wireless access points to access the internet. If a situation requires that the laptop have access to the Town's network resources, IT needs to be contacted so that appropriate configuration changes can be made. We will also verify that anti-virus software is up-to-date and that Windows updates have been applied so as not to infect the network.

15. Switches and hubs are used to extend our network capability when there are not enough wall ports available. Only devices programmed by IT should be connected into a switch or hub. If in doubt, do not connect.

16. Equipment cabinets and rack mounted devices are located in various building locations. These typically house our larger power supplies and wide-area network switches. Many of these switches provide primary communications across our fiber network. These devices should not be touched

17. Vendors contracted to do IT related work or any type of hardware installation must contact IT first before installing anything on the network. We will work with the vendor to ensure their system is compatible with our infrastructure and that the implementation is scheduled to minimize disruption.

18. Uninterruptable Power Supply Units (UPS) are used to provide battery-backup power and surge protection to electronic devices. Do not plug heating and cooling units or printers into a UPS without consulting IT. UPS's can trip like any electrical circuit when overloaded.

VII. Employee Responsibility

Use of the Internet and E-mail system is a privilege and is not to be abused. Employees shall comply with all applicable sections of this policy in addition to the following:

When sending e-mail messages, employees are representing the Town of Nantucket and are responsible for the content of all messages. Each employee is expected to ensure that the information being entered or sent is not offensive, frivolous or inappropriate. An employee should never forward any inappropriate email for any reason. Although spam and viruses can be an unfortunate consequence of internet and email use, every precaution should be made, including but not limited to the following:

a) Do not open email from anyone you do not know. If you are in a department that must do so to provide information and the email content looks suspicious, do not click on any embedded links and contact the Information Technology Department;

b) Do not forward email or files unless you are confident of their source;

c) Do not use the internet for any unnecessary reasons. Do not provide your town email account to anyone other than for Town business.

Due to bandwidth limitations, employees are prohibited from playing or using radio or streaming video over the internet unless specifically approved for town business.

Personal use of a Town computer must be limited in duration and frequency so that it does not interfere with the employee's work responsibilities or adversely affect the productivity of the employee or the employee's co-workers.

Employees are expected to cooperate fully in the investigation of any complaint or alleged violation of this policy. Informal guideline employees are advised to follow with regard to the appropriateness of internal and external email messages and Internet access is: ***Is it appropriate for the front page of the newspaper?***

VIII. Management Responsibility

Department Heads and supervisors are responsible for ensuring that staff understand and adhere to this policy.

IX. Violations of this Policy

Violations of this policy will be handled in a manner consistent with the Town's disciplinary process up to and including termination; and, may be subject to prosecution by local, state and federal authorities.

X. Town Limitation of Liability

The Town shall not be responsible for the accuracy or quality of information obtained through the Internet; financial obligations arising through the unauthorized use of the Internet; any illegal use of the Internet by Town employees.

The Town reserves the right to restrict or terminate an employee's access privileges at any time for any reason.

The Town has the right to monitor computer usage activity in any form that it sees fit to maintain the purpose of this policy.

This policy is subject to revision at any time by the Town Manager.

End