

Town of Brunswick



Computer Use Policy

Town of Brunswick Computer Use Policy

Table of Contents

1.	General	1
2.	Access	1
3.	Acceptable Use	1
4.	E-Mail	1
5.	E-Mail Attachments	2
6.	Internet & Websites	2
7.	Privacy	3
8.	Security	3
9.	Personal Use	3
10.	Copyrights	4
11.	Other Prohibited Uses	4
12.	Breaches of Policy	4
13.	Amendments	5
14.	Employee Acknowledgement	5
15.	Definitions	5
	Approved Software	6
	Computer Use Acknowledgement Form	

Town of Brunswick Computer Use Policy

1. General

The Town of Brunswick has adopted this policy to provide its employees with the general requirements for using the Town's computers, networks, internet services and e-mail services.

2. Access

The level of access employees have to computers, networks, internet services and e-mail services is based upon specific job requirements. Employees must have approval of a department head in order to gain access to the Town's computers, systems or services. The system administrator must also approve access before an employee is authorized to use any of the Town's computers, systems or services. Without the approval of a department head and the system administrator, access shall not be granted.

3. Acceptable Use

Employee access to the Town's computers, networks, internet services and e-mail services is to aid employees in the performance of their employment responsibilities. Unless specifically allowed elsewhere in this policy, any use not consistent with this purpose is prohibited.

4. E-Mail

E-mail has been provided to assist and enhance communication. All e-mail accounts must be approved by the system administrator. Unless an exception is approved by the system administrator, the use of free commercial accounts such as Yahoo, Hotmail and the like is prohibited for both professional and personal use. All accounts must be accessed using an e-mail program approved by the system administrator.

It is not necessary for an e-mail to contain an attachment in order to deliver a virus. Viruses can be transmitted simply by opening infected mail. Because preview panes and auto-preview functions work by opening the mail, those features shall be disabled on all computers and systems. Further, employees should not open mail from sources unfamiliar to them.

Employees are cautioned that e-mail is considered a public record under Maine's Freedom of Access law. Employees should assume that any e-mail may be deemed "public information" and treated the same as any other written communication. Precautions should be taken to preserve important communications in hard copy form. Consideration should be given to archiving e-mails to media for permanent storage.

Employees are cautioned that deliberative discussions via e-mail could be construed to be a public meeting under Maine's Freedom of Access law.

Employees are cautioned to avoid using e-mail and other mediums to promote, advocate or communicate personal views or the views of other individuals or organizations that could be perceived as an endorsement by the municipal government of the Town when no such endorsement has been provided.

Employees shall not make the name and e-mail addresses of other employees available to those whose intent is to communicate with employees for purposes unrelated to their job responsibilities.

5. E-Mail Attachments

E-mail attachments are a very common method of spreading viruses. Every e-mail attachment should be treated as suspect. Even when the sender is known, an e-mail and its attachment should not be opened without first confirming its legitimacy and content with the sender. Further, even if an e-mail is received from a known sender and the legitimacy of it and its attachment has been confirmed, recipients should proceed with caution. The sender may not have the same level of virus protection as the Town. Many senders unknowingly spread viruses by forwarding innocent appearing attachments received from other trusted sources. As an additional precaution, every attachment should be scanned using virus protection software prior to opening it. Employees should remember however, that virus protection software will only detect viruses with known definitions that have been loaded on the computer system. If there is no definition loaded to the system because the virus is relatively new or because the system has not been properly updated, the anti-virus software will not detect the virus.

Employees should not open an image that the sender hasn't created personally. Employees should not open any attachment that is in the form of an executable file. An executable file is a file that will run a program on your computer. Often, but not always, executable files contain the ".exe" file extension. Employees should be guided by the basic rule, "when in doubt, don't."

6. Internet & Websites

Internet access is provided primarily for research in connection with an employee's specific job duties. Employees are reminded that use of the internet must not interfere with an employee's job duties. Without the approval of a supervisor, "surfing the net" is considered an unproductive use of the resource and an employee's time.

Only software approved by the systems administrator may be used to browse internet websites. Employees are encouraged to exercise care in selecting websites to visit on the internet, including sites received in, or linked from, e-mail. Viruses can be transmitted simply by viewing a site that contains computer code written to transmit viruses to others.

Employees shall not use internet services and access for streaming media applications without requesting and receiving permission from the system administrator. Permission may only be granted on a limited basis for limited durations.

7. Privacy

The Town of Brunswick retains control, custody and supervision of all computers, networks, internet services and e-mail services. Employees waive and have no expectation of privacy in their use. The Town reserves the right to at any time to inspect and/or monitor computer system files, logs and other activity including e-mails stored on any server or individual computer. Monitoring may also include surveillance programs designed for that purpose.

8. Security

The Town employs various measures to protect its equipment and data from deliberate or inadvertent destruction or misuse. Such measures include the designation of individual accounts, log-ins, and passwords. Sharing of accounts, log-ins and passwords is prohibited unless the system administrator grants an exception. Passwords shall be safeguarded and not divulged. If it is necessary to maintain a written copy of a password, that copy shall be placed in a secure location. When employees are required to choose a password, they shall refrain from selecting a password that may easily be linked to the employee such as birth dates, children's names, etc.

The Town also uses a variety of other means to protect its systems and data including security settings in software applications, virus scanning software and firewalls. Employees shall not alter, or attempt to alter, any security setting without the approval of the system administrator including those set within software applications. Employees shall not disable virus protection or attempt to bypass firewall protections without the approval of a system administrator.

9. Personal Use

Diminimus personal use of the Town's computers, networks, internet services and e-mail services is permitted so long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. Such personal use must be consistent with appropriate professional conduct. Employees are reminded that all personal use must comply with this policy as well as all other procedures, regulations and laws. Employees are further reminded that all use may be monitored and inspected.

Employees shall not install, or attempt to install, on any Town computer or system, personally owned software or shareware downloaded from the internet.

Any use of the Town's equipment or services for private financial gain, commercial advertising or solicitation purposes is prohibited.

10. Copyrights

It is the policy of the Town of Brunswick to fully comply with all laws pertaining to the reproduction, use or distribution of copyrighted or otherwise protected materials. The Town will comply with all licensing requirements. Employees shall not install, or attempt to install, any software on any computer or system unless the Town is properly licensed and approval is obtained from the system administrator. Employees shall not make copies of software other than those copies authorized in the software license. Employees shall respect the copyrighted protection of materials found on the internet.

11. Other Prohibited Uses

Any use that is determined to be inconsistent with this policy or other policies, rules or regulations of the Town of Brunswick is prohibited. In addition to the prohibited uses cited throughout this policy, other prohibited uses include but are not limited to:

- a. Any use that is illegal.

- b. Any use involving materials that are obscene, sexually explicit or sexually suggestive.
- c. Any use that represents personal views as the views of the Town of Brunswick.
- d. Malicious use or deliberate disruption of the Town's computers, networks, internet services or e-mail services and/or breach of security features.
- e. Misuse or deliberate damage to the Town's computer systems and/or components.
- f. Copying, downloading, installing/removing software or applications without the approval of the system administrator.
- g. Failing to report a known breach of computer security to a system administrator or supervisor.

12. Breaches of Policy

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Violations of the policy that are also violations of law may result in referral to law enforcement authorities. Employees who violate this policy may also be required to compensate the Town for any damages or costs whether direct or as a consequence of the failure to adhere to this policy. The Town will not make job accommodations to individuals who have, by virtue of inappropriate conduct, lost the privilege of using the Town's computers, systems, internet services or e-mail services.

13. Amendments

The Town may amend and supplement this policy from time. Employees will be provided with any amendments and supplements are expected to abide by them.

14. Employee Acknowledgement

Each employee and any other person authorized to use the Town's computer or its systems, are required to sign an acknowledgement indicating that the employee or other authorized user has read this policy and agrees to abide by it. The acknowledgement will be filed in the employee's personnel file and/or maintained by the systems administrator.

15. Definitions

System Administrator – The person designated by the Town Manager to be responsible for the overall operation and use of computers, networks, internet service and E-mail services. Individual networks may have different systems administrators. Internet and E-mail services shall have one system administrator who may delegate certain duties to qualified employees.

Town of Brunswick Approved Software

Web Browsers

Microsoft Internet Explorer

Netscape Navigator

E-Mail

Microsoft Outlook

**Town of Brunswick, Maine
28 Federal Street
Brunswick, Maine 04011**

Computer Use Policy Acknowledgement

I acknowledge that I have received, read and understand the Town of Brunswick's policy regarding computer use and agree to abide by its provisions. I understand that my failure to adhere to the policy could result in my being denied access to the Town of Brunswick's computers, networks, internet services or e-mail services. Further, I understand that failure to adhere to the policy could also result in disciplinary action being taken against me.

Signature

Date

Printed Name