


<b>TOWN OF WOODFIN – POLICY STATEMENT</b>		Policy #:	
Department: Administration / Finance		Issuing Date:	06/20/2017
	Policy Title:  <b>IT Acceptable Usage Policy</b>	Effective Date:	06/16/2021
		Revised Date:	06/20/2017
		Prepared By:	Jason Young, Town Administrator
		Approved By & Date:	Board of Commissioners 06/20/2017

**PURPOSE:** This document establishes the Town policy for the proper use of all Town information technology including, but not limited to computer systems and their attached peripherals, laptop computers, phones, cellular phones, beepers, faxes, smartphones, voicemail systems, e-mail systems, network resources, and internet resources.

**POLICY:** All technology resources owned by Town of Woodfin are in place to enable the Town to provide its services in a timely and efficient manner. Any activity or action that interferes with this purpose is prohibited. Because technology systems are constantly evolving, Town of Woodfin requires its employees to use a commonsense approach to the rules set forth below, complying not only with the letter, but also the spirit of this policy. Appropriate use of this technology must reflect Town standards and be legal, ethical, and show restraint in the consumption of shared resources.

**DEFINITIONS:**

**Client** – The computer “end user” or actual PC workstation connected to the server in a network environment.

**Computer Virus** – A malicious computer program designed to interfere or harm normal daily computer operations.

**Data Streaming** – A technique of transferring data in a steady and continuous flow. Typical applications are for accessing audio and/or video. Since the flow of data is constant and ongoing, this process has the potential to slow the response time of the entire network.

**Desktop Themes** – A set of programs typically downloaded from the internet that can change many attributes of your computer screen.

**E-Mail** – The distribution of messages, documents, files, software, or images by electronic means. This includes internal e-mail, external e-mail, and internet e-mail.

**Encryption** – A security method of using a computer program to scramble a message to hide its contents.

**Firewall** – A security system used to prevent unauthorized access to Town of Woodfin’s computer servers, networks, and clients.

**Internet (or the World Wide Web)** – A public electronic medium through which information and electronic mail travels.

**Public Domain Software** – Computer systems that do not retain any copyright claims. The authors of these programs want computer users to have them free of charge.

**Server** – A central computer or device that connects computers on a network allowing users to share services as well as data.

**Smartphone** – A mobile phone that includes advanced functionality beyond making phone calls and sending text messages. Typical smartphone functionality includes the ability to synchronize email messages, calendar and contact information with Town of Woodfin's email system.

**TCP/IP** – Abbreviation for Transmission Control Protocol/Internet Protocol, which is the communication protocol utilized by the majority of computer networks.

**Work Response Time** – Also known as user response time, it is the time it takes a computer to interact with the network server.

- RESPONSIBILITIES:**
- A. Department Supervisors are responsible for their staff complying with all provisions of this technology usage policy, and to investigate in a timely manner, document and report any alleged or suspected non-compliance to their department head.
  - B. All non-compliance documentation should be sent to the Town Administrator by way of the Department Head.
  - C. Employee use of the Town of Woodfin information technologies is a revocable privilege. User accounts and password access may be suspended or permanently revoked based on violations of this information technology usage policy. Violations may also result in disciplinary action up to and including termination in accordance with ARTICLE VIII. SEPARATION, DISCIPLINARY ACTION, AND EMPLOYEE APPEALS of the Town of Woodfin Personnel Ordinance. Severe violations of this policy may also result in employee criminal prosecution and/or civil liability.

- PROCEDURE:**
- A. Information Access and Ownership
    - a. All technology resources and all information transmitted by, received from, or stored on Town of Woodfin systems are the property of Town of Woodfin and as such, are subject to inspection by Town officials. The Town reserves the right for business purposes to enter, review, and monitor the information on all systems, including voice mail, electronic mail, and information stored on computer systems or media without advance notice. This might include investigating theft, unauthorized disclosure of business, proprietary, of personal information, personal abuse of the system, or monitoring workflow and productivity.
  - B. Security
    - a. Each user is responsible for all actions taken while using their profile, password, or access code. Great care must be taken by all employees to follow appropriate security procedures to protect the rights of our citizens with regard to unauthorized access of sensitive and confidential data.
  - C. Account Access
    - a. Employees may only access accounts for which they are authorized and take reasonable precautions against unauthorized access to their accounts. Employees may not share a password and should always log off of their PC, or lock their computer when it is unattended. Each user will be held responsible for the actions taken by his or her assigned user id(s) on any Town electronic system.
  - D. Honest Representation
    - a. Each user shall identify themselves honestly, accurately, and completely when using any technology media. This includes telephone, email, social media, on-line user groups, or when setting up computer accounts. Only those employees who are authorized to speak or write to the media on behalf of Town of Woodfin may do so, even in a casual user group or chat room. Chat and newsgroups are strictly limited to Town business need purposes. This rule shall not apply to law enforcement activities wherein it is considered advantageous to the Department to disguise or misrepresent the sender or origin of such communications to assist in the investigation of crimes or suspected crimes.

E. Copyrighted Material

- a. Employees should always assume that information on the internet is copyrighted unless otherwise indicated. Users who download and use copyrighted material must be in compliance with current copyright laws. The Federal Copyright Act 17 U.S.C. 101 et. Seq., (1988) protects and prohibits misuse of all original works of authorship in any tangible medium of expression. Most State and Federal Government documents contain a statement of permission to copy.

F. Electronic Mail Appropriate Usage Guidelines

- a. E-mail is considered an official form of communication between departments and employees. Computer users must check for the receipt of e-mail messages each working day, except while on vacation or those days designated official Town holidays. On days taken as personal time off, employees should employ the “out of office” message.
- b. Sending large attachments to outside addresses can dramatically affect the internet connection for the entire infrastructure. Consider the need, and if deemed appropriate, have a drop box or similar secure file transfer appliance where the recipient will be able to retrieve it.
- c. Any e-mail to an address outside of the Town of Woodfin domain will be traveling across the internet, and therefore should be considered public domain. You should refrain from sending confidential or sensitive information by these means unless proper, formalized security tools (such as encryption) have been established. It is the responsibility of each department and user to protect confidential and sensitive information where intentional, inappropriate, or accidental disclosure of the information might expose the Town or an individual to loss or harm.
- d. Users shall not automatically forward a Town e-mail account to an internet email address. This practice may jeopardize the confidentiality and integrity of Town e-mail messages. It also can give the sender a false sense that the message is protected by internal e-mail systems. Electronic services created by Town administrators are exempt. Additionally, users are not allowed to access third-party e-mail services to conduct Town business without prior approval from their immediate supervisor or department head.
- e. Users must always protect the privacy and confidentiality of others.
- f. Users must delete and purge all unnecessary mail that does not require retention.
- g. Users must be courteous and follow accepted standards of etiquette.

G. Electronic Documents/Email Privacy and Usage Guidelines

- a. Electronic Documents: Any document created or stored on an electronic computing device is considered an “electronic document” and is subject to all privacy and data retention statutes of North Carolina. Files created in Word, Excel, Access, Power Point, and Visio are examples of electronic documents. Although e-mail is considered a temporary communication, the content of e-mail is still subject to N.C. Gen. Stat. § 121-8 and N.C. Gen. Stat. § 132-1.
- b. Privacy: To the greatest extent possible, effort has been made to preserve all employees’ individual privacy. However, Town of Woodfin computer systems and networks are public property and subject to the North Carolina Public Access statutes. Employees therefore should have no reasonable expectation of privacy in the use of these resources. Town of Woodfin reserves the right to trace and document any email generated by Town provided resources. Emails not subject to public access containing sensitive or confidential information should have the

following statement on the subject line of the document address: "CONFIDENTIAL" or "CONFIDENTIAL SUBJECT TO GENERAL STATUTE." If this is done, the IT department is not required to release the information without proper legal directive.

- c. Not all "official" records are open to the public: Many records are protected from general access or casual reference on a "need to know" basis by federal or state laws, or by legal precedent, and can only be seen by a court order. Therefore, certain records should be considered confidential to protect the privacy rights of employees and the general public. Employees should consult with their department Supervisor prior to releasing any information.

#### H. Data Protection

- a. Town of Woodfin uses internet firewalls, virus protection, data encryption, and other mechanisms to ensure the safety and security of all data. Any employee who attempts to circumvent these mechanisms, or who knowingly propagates any computer virus into the system may be subject to disciplinary action in accordance with ARTICLE VIII. SEPARATION, DISCIPLINARY ACTION, AND EMPLOYEE APPEALS.

#### I. Standard Practices—Equipment Safety

- a. All electronic equipment shall be maintained and cared for in an appropriate manner. If personal negligence should cause the equipment to become lost or stolen, the user may be held financially responsible.
- b. The Town will consider negligence on a case-by-case basis. In addition, the user should consider the following guidelines:
- c. All users assigned a laptop computer or handheld device will be personally liable for the care and condition of the equipment.
- d. Computers are sensitive to extreme temperatures. This includes external hard drives, CD-ROMs, batteries, disks, etc. Safeguard equipment appropriately during times of extreme heat or cold.
- e. Laptops, handheld devices, and associated materials are to be transported in appropriate carrying cases when available to ensure safety.
- f. Users must exercise care at all times to preclude theft. Portable devices such as laptop computers, handheld devices, memory sticks, etc. should not be left unattended when outside of Town facilities. Should an electronic system be lost or stolen, the responsible user must contact the Town Administrator immediately.
- g. All users must be aware of the damage that a malicious application (i.e., virus, worm, Trojan horse, etc.) can cause the Town's electronic systems. Report suspected incidents immediately to the department head.

#### J. Sexually Explicit Material

- a. Employees shall not access, store, or distribute any electronic media that contains pornography or sexually explicit material. Such prohibition shall not apply to law enforcement officers conducting a specific investigation if such material is pertinent in the opinion of the Department Head. Law enforcement officers are expected to receive prior authorization in all but the most extreme circumstances from their supervisor to access sexually explicit material to determine if gathering or reviewing such information is integral to the investigation.

#### K. Harassment

- a. No employee shall use any Town electronic medium to libel, slander, harass, or threaten another person.

- b. It is also against Town policy to send the following:
  - i. Unsolicited e-mail advertising (SPAM) or junk mailings
  - ii. Chain letter emails/Solicitation of funds
  - iii. E-mails containing fake or anonymous e-mail addresses
  - iv. E-mails containing jokes, stories, or material unrelated to Town business
  - v. E-mails that contain profanity, obscenity, or discriminatory remarks
- c. Any Town employee who violates the provisions of 6.10, 6.11, or 6.11.1 thru 5, may be subject to disciplinary action in accordance with ARTICLE VIII. SEPARATION, DISCIPLINARY ACTION, AND EMPLOYEE APPEALS.

L. Unnecessary or Unlawful Usage of the Internet

- a. Excessive personal internet usage causes network and server congestion. It can slow down other employees work response time and it consumes shared resources. Each computer may be configured to allow screening and review of the web sites visited on the internet. Employees should understand that when they log onto the internet through the Town infrastructure that their movement on the internet may be logged and tracked. Unlawful internet usage may also create negative publicity for the Town and expose us to significant legal liabilities. Any Town of Woodfin employee who knowingly uses the internet or intranet unlawfully may be subject to disciplinary action in accordance with ARTICLE VIII. SEPARATION, DISCIPLINARY ACTION, AND EMPLOYEE APPEALS.

M. Personal/Political Business

- a. Political advertising, campaigning, or personal commercial business is strictly forbidden on Town resources.

N. Downloading or Uploading Licensed Software

- a. No software may be installed, copied, or used on Town computers without the involvement of the department head or his or her designate. Software subject to licensing must be properly licensed, and all license provisions must be strictly obeyed.

O. Configuration of Town Computers

- a. Employees may not modify the software configuration of their computers other than to change their screen resolution, wallpaper, and screen saver settings. Employees should exercise common sense and caution in determining what programs, apps, and other software to download to Town Computers. Employees are required to surrender passwords and access keys to their department head. Modification of passwords and or access keys without communicating such changes to the Department head may result in disciplinary actions up to and including termination.

P. Employee Termination

- a. Employees who are terminated have no rights to the content of their e-mail messages and will not be allowed access to the e-mail system. A terminated employee who files a grievance procedure in a timely fashion in accordance with the provisions of ARTICLE IX. GRIEVANCE PROCEDURE and believes information contained in their e-mail account to be relevant to said procedure may request in writing that the Town Administrator authorize access to said information. The Town Administrator may grant such a request if the information is not deemed detrimental to the interests of the Town.

**SCOPE:** This policy applies to all employees of the Town of Woodfin.

**COMMENTS:** Policy should be reviewed annually and updated, as necessary.

**POLICY  
AUTHORITY:** Please contact the Town Administrator at 828-253-4887 with any questions pertaining to this policy.