

Town of Randolph Acceptable Use Policy for Computer Systems

Introduction

This Acceptable Use Policy sets forth the principles that govern the use of the Town of Randolph (Town) computer system by its employees. This policy is designed to help protect the Town and its computer system, from irresponsible, abusive or illegal activities by employees.

1. Definitions

For purposes of this section, computer system means all computer-related components and equipment including, but not limited to, host computers, file servers, workstation terminals, laptops, software, internal or external communication networks, the world wide web (www), the Internet, commercial online services, bulletin board systems, back up systems and the internal and external e-mail systems accessed via Town computer equipment.

2. Disclaimer

The Town cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic resources and communications are warned that they may come across or be recipients of material they find offensive.

3. Internet and Email Access

- a. Transmission of electronic messages on the Town computer system shall be treated with the same degree of propriety, professionalism, and confidentiality as written correspondence. The following are examples of uses of the Town computer system which are prohibited:
 - i. Communications that in any way may be construed by others as disruptive, offensive, abusive, discriminatory, harassing, or threatening;
 - ii. Communications of sexually explicit images or messages;
 - iii. Transmission of chain letters or solicitations for personal gain, commercial or investment ventures, religious or political causes, outside organizations, or other non job-related solicitations during or after work hours;
 - iv. Access to Internet resources, including web sites and news groups, that are inappropriate in a business setting;
 - v. Any other use that may compromise the integrity of the Town and its business in any way.
- b. Email messages that are intended to be temporary, non-substantive communications may be routinely discarded. However, employees must recognize that emails sent, received, or stored on the Town computer system are subject to Vermont's Public Records Law and may be covered by the State of Vermont's retention schedule for municipal records.

4. Computer Access

- a. The Town computer system is to be used by employees for the purpose of conducting Town business. Occasional, brief, and appropriate personal use of the Town computer system is permitted, provided it is consistent with this policy and does not interfere with an employee's job duties and responsibilities.
- b. Employees should have no expectation of privacy regarding anything created, sent or received on the Town computer system. The Town may monitor any and all computer transactions,

communications and transmissions to ensure compliance with this policy and to evaluate the use of its computer system. All files, documents, data and other electronic messages created, received or stored on the Town computer system are open to review and regulation by the Town and may be subject to the provisions of Vermont's Public Records Law.

- c. Employees may not introduce software from any outside source on the Town computer system without explicit prior authorization from their supervisor. Employees may be held responsible for any damages caused by using unauthorized software or viruses they introduce into the Town computer system.
- d. Employees who have a confidential password to access the Town computer system should be aware that this does not mean the computer system is for personal confidential communication, nor does it suggest that the computer system is the property of that person.

5. Prohibited Usage

Prohibited usages include, but are not limited to:

- a. Using computer and network resources for illegally downloading or sharing music, movies, software or other files, or other non-Town related applications
- b. Sending harassing messages; sending frivolous or excessive messages, including chain letters, junk mail, spam, and other types of broadcast messages, either locally or over the Internet; using excessive amounts of storage
- c. Launching computer attacks, probes, or otherwise attempting to subvert the security of any system or network at the Town or on the Internet
- d. Intentionally or irresponsibly introducing any computer viruses, worms, Trojan Horses, spy ware, or other rogue programs or malware to hardware, software, systems or networks at the Town or on the Internet; or physically damaging systems.

Adoption

Adopted by the Legislative Body on the 19th day of February, 2008.

LEGISLATIVE BODY

(Typed Name)	(Signature)
James Hutchinson (Chair)	/s/ James Hutchinson
Lawrence Townsend (Clerk)	/s/ Lawrence Townsend
Stephen Springer	/s/ Stephen Springer
Kenneth Goss	/s/ Kenneth Goss
Damon Lease	/s/ Damon Lease