

POLICY NO.: 82
DATE ADOPTED:

TOWN OF SPENCER BOARD OF SELECTMEN POLICY

Policy on the Use of Information Technology Resources (ITR)

Purpose of this Policy

This document formalizes the policy for employees and users of all Town of Spencer's Information Technology Resources (hereinafter referred to as ITR), including computers, printers, and other peripherals, programs, data local and wide area networks, e-mail and the Internet. Use of Town of Spencer's ITR by any employee or user shall constitute acceptance of the terms of this policy and any such additional policies.

This document will be handed out by Human Resources (HR) to all new employees. A signed copy of the form at the end of this document acknowledging the receipt and understanding of this policy will be kept on file with HR. This document may be routinely updated, following approval by the Board of Selectmen, and placed on the Town's Public drive under IS/ISPOL.DOC. An e-mail will be sent to all employees indicating when there has been a change in the document and it is the responsibility of the employee to review the revised document located on the P drive.

The purpose of this policy is to accurately convey the policies of the Town in the use of the Town of Spencer's ITR. The policies contained within this document reflect a responsible use of the Town's ITR. The policy will be strongly enforced and employees and users of the Town of Spencer's ITR are expected to follow this policy at all times.

This policy is designed to protect the Town of Spencer and its employees as well.

Other laws also cover certain subjects noted in this policy, some of which are not only forbidden under this policy but are also serious crimes, potentially involving substantial fines and jail terms. Nothing in this policy lessens your responsibility under those laws.

Exception for Police Department, Fire Department & Library: It should be noted that the Police and Fire Departments shall maintain separate ITR policies due to the unique operations associated with ITR and that the Library shall maintain a separate ITR policy due to public access to ITR.

User Responsibility

It is the responsibility of any person using the Town of Spencer's ITR to read, understand, and follow this policy. In addition, users are expected to exercise

reasonable judgment in interpreting this policy and in making decisions about the use of ITR. Any person with questions regarding the application or meaning of this policy should seek clarification from the Town's Information Systems (IS) or HR Department.

Failure to observe this policy may subject individuals to disciplinary actions, as determined by the Town Administrator, in accordance with collective bargaining agreements and employment laws as applicable.

Acceptable Uses

The Town of Spencer firmly believes that ITR empowers users and makes their jobs more fulfilling by allowing them to deliver better services at lower costs. As such, employees are encouraged to use ITR to the fullest extent in pursuit of their departmental goals and objectives.

Unacceptable Uses of Town of Spencer's ITR

The following is a listing of unacceptable uses of the Town of Spencer's ITR:

- In furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether local, state or federal;
- For any political purpose;
- For any commercial purpose;
- To send threatening or harassing messages, whether sexual or otherwise;
- To access or share sexually explicit, obscene, or otherwise inappropriate materials;
- To infringe any intellectual property rights;
- To gain, or attempt to gain, unauthorized access to any computer or network;
- For any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
- Bandwidth compromising programs are not allowed without prior approval. Examples include but are not limited to streaming video and audio (watching video or listening to music), remaining on web cams for non-business functions is prohibited, online gaming and the like;
- To intercept communications intended for other persons;
- To misrepresent either the Town of Spencer or a person's role at the Town of Spencer;
- To distribute chain letters;
- To access on-line gambling sites;
- To libel or otherwise defame any person;
- Installation of ANY software or hardware not approved by IS, the Town Administrator, or the appropriate department head. IS is responsible to comply with the Commonwealth of Massachusetts, Chapter 30B Bidding practices with respect to the Town's purchase of any and all ITR equipment. ALL software and hardware or related ITR equipment must go through IS to ensure the Town's compliance with state laws. IS is also responsible for maintaining accurate asset information regarding all ITR.

Data Confidentiality

In the course of performing their jobs, Town of Spencer employees and users often have access to confidential 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 by their job. Under no circumstances may employees or users disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs.

Copyright Protection

Computer programs are a valuable, intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. **Software cannot be copied or installed without a valid license obtained through IS or the appropriate department head.**

In addition, employees are not allowed to install personally owned hardware and/or software on a Town of Spencer ITR without express authorization from the IS Department or Town Administrator and the appropriate department head. The installation of such software on a Town of Spencer's machine may be in violation of licensing infringements, or may introduce other problems associated with network access, hardware performance, etc.

Computer Viruses

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the Town of Spencer's network. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any source other than the vendor or IS. It is a good practice to scan portable storage devices periodically to see if they have been infected. Users should not interfere with virus scanning software that is installed on their computers. Copy all "outside" documents to one of your network drives prior to opening. That process will automatically scan the file and alert you should the file contain a virus.

Network Security

Most desktop computers are connected to a local area network, which links computers within the Town of Spencer and through the wide area network, to other computers within the organization. As such, it is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users should never share their passwords with anyone else, and should promptly notify the IS Department if they suspect their passwords have been compromised. In addition, users

who will be leaving their PC's unattended for extended periods should log off the network or "lock" their machines during this time.

Website

Access to websites is restricted to work related sites with an exception allowed during non work time such as morning and afternoon breaks.

E-Mail

When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message (username@spencerma.gov), users should consider e-mail messages to be the equivalent of letters sent on official letterhead. For the same reason, users 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 should not write anything in an e-mail message that they would not feel comfortable putting into a letter.

Subject to certain exceptions in the law, employees are reminded that e-mail messages are considered public records, copies of which may be requested by any member of the public. It should be noted that even deleted messages might be subject to disclosure because they still exist on backup tapes.

Furthermore, because of the electronic search and retrieval methodologies available with e-mail, there is a much higher degree of likelihood that a carelessly composed message containing an unforeseeably relevant key word will turn up in some notorious and embarrassing context. Users must keep this constantly in mind.

E-mail attachments represent an impact on network capacity and should only be used to communicate official business documents to recipients. The forwarding of non-business related information is in violation of this policy. Employees who are the recipients of non-business e-mail are required to discard them. E-mail attachments that are received from an unknown party should be considered "suspicious" and should not be opened until the sender's identity can be confirmed. Many viruses are spread using e-mail systems in this manner.

The Internet offers a wide variety of electronic mailing lists. These mass-mailing lists come from list servers managed by a wide range of organizations. To receive the mass-mailings one must subscribe to the list using the Internet e-mail address. Employees are NOT to subscribe to mailing lists if the content is not directly related to their job function. Recreational examples would include "Joke of the Day," "Horoscopes," "Trivia," "Daily Word," etc. Each of these mass-mailings uses network storage capacity that should be used for other business related purposes.

No Expectation of Privacy

Town of Spencer's ITR are the property of the Town of Spencer and are to be used in conformance with this policy. The Town of Spencer retains the authority to inspect any user's computer, and data contained in it and data sent or received by that computer. Use of Town of Spencer's ITR constitutes express consent for the Town of Spencer 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.

Requests of IS

Requests for new hardware, software, and applications development must come through IS with department head approval and following proper procurement procedures.

Help Desk Procedures

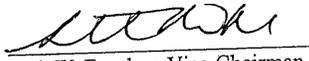
Employees/Users requiring assistance with software, hardware, applications or any issues related to ITR are required to call the IS Administrator for assistance with approval from their respective department head. A work ticket will be opened by IS. If there are multiple open tickets they will be prioritized and worked on in priority order.

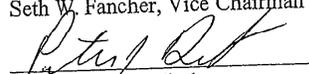
Please return this signed acknowledgement to the Information Systems Department, acknowledging that you have read and understand the policy put forth in this document. This signed acknowledgement will be forwarded to Human Resources to become part of your personnel file and a copy will be kept on file in the IS Department.

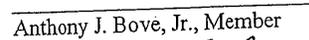
Adopted by the Town of Spencer Board of Selectmen:

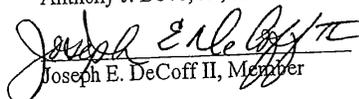
Date: 5-10-10


Donald R. Berthiaume, Jr., Chairman


Seth W. Fancher, Vice Chairman


Peter J. Durant, Clerk


Anthony J. Bove, Jr., Member


Joseph E. DeCoff II, Member

I have read and understand the Town of Spencer's Information Technology Resources (ITR) policy.

Print Name: _____ Date: _____

Signature: _____

**TOWN OF SPENCER
POLICY ACKNOWLEDGEMENT RECEIPT**

_____ **Summary of Conflict of Interest Law for Municipal Employees**

_____ **Sexual Harassment Policy**

_____ **Use of Information Technology Resources (ITR) Policy**

Employee Signature

Date

