



Town of Shirley Technology Acceptable Use Policy

Mission Statement

The Town of Shirley is committed to the use of electronic resources and technology to enhance the ability for Town employees to accomplish their jobs. Therefore, all employees are encouraged to utilize these resources within the guidelines set forth in the Acceptable Use Policy.

The Acceptable Use Policy addresses the ethical and appropriate use of technology resources, the security of the network, and the safety of employees, students and the public. Although there is a belief in intellectual freedom and access to information, reasonable precautions will be taken to limit access to controversial and/or offensive materials by:

- Using software and/or hardware that may block the materials; and
- Training users to appropriately use technology and access information.

The ultimate responsibility for a user's actions rests with the user.

This policy applies to all town employees acting in the performance of Town of Shirley municipal business.

Responsibilities of Town Employees

- Learn and follow the guidelines set forth in this Acceptable Use Policy.
- Return an application form signed by the user stating the user has read, understands, agrees and will adhere to all guidelines and assume responsibility for their own actions.
- Use the Internet, telephone system, computers, and e-mail for work-related or educational functions only.

Guidelines for Use of Technology Resources

Acceptable Use

Computers, telephones and networks are to be used in a responsible, efficient, ethical and legal manner and must be in support of the performance of Town of Shirley business. Incidental personal use of technology such as E-mail is permitted but subject to monitoring. Transmission of any material in violation of any federal or state regulation is prohibited.

Unacceptable Use

This includes, but is not limited to, the following:

- Giving out personal information about another person, including financial, credit or other confidential information is strictly prohibited.
- Any use of the network for commercial or for-profit purposes is prohibited.
- Any use of the network for product advertisement or political lobbying is prohibited.
- Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.

- No use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.
- Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
- Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network.
- The unauthorized installation of any software, including shareware and freeware, for use on Town of Shirley computers is prohibited. The only exception to this rule is Active X controls used by Microsoft Internet Explorer version 7 or later.
- Use of the network to access or process pornographic material, inappropriate text files (as determined by the System Administrator or Town Administrator/Board of Selectmen, or files dangerous to the integrity of the local area network is prohibited. Note: The Shirley Police Department may need to access inappropriate websites or materials during the course of investigation. This is not considered a violation of this rule since it is done in the performance of their job.
- The Town of Shirley network may not be used for downloading entertainment software or other files not related to the mission and objectives of the Town of Shirley for transfer to a user's home computer, personal computer, or other media. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the Town of Shirley business.
- Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).
- Use of the network for any unlawful purpose is prohibited.
- Use of profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited.
- Establishing network or Internet connections to live communications, including voice and/or video (relay chat) for recreational use is prohibited.
- Playing online recreational computer games is prohibited.

Content Filtering

The Town of Shirley will initiate content filtering at firewall level. Content filtering is not 100%; please report any problems with this service to the System Administrator.

E-mail

E-mail accounts are provided to Town of Shirley employees after signing the Acceptable Use Policy. Those currently holding e-mail ID will have same withdrawn for failure to sign the Acceptable Use Policy.

Unacceptable use of e-mail includes, but is not limited to:

- Messages relating to or in support of illegal activities.

- SPAM/Mass e-mails.
- Chain letters.
- Mail for solicitation purpose.
- Mail involving commercial, political or religious content.

Electronic mail is not private; system operators, hiring authorities and authorized supervisors have access to all e-mail, which may be considered a public record under Massachusetts state law.

Network Etiquette Rules

These rules include, but are not limited to, the following:

- Be polite.
- Use appropriate language—swearing, using vulgarities or any other abusive language is inappropriate.
- Caution should be used when revealing your personal address or telephone number or those of anyone else.
- Caution should be used when revealing credit or checking account information or social security numbers across the Internet.
- Do not disrupt network functions.
- Do not attempt to gain unauthorized access to system programs or computer equipment.

Network Security

After signing the Acceptable Use Policy, users will be assigned a username and password to access Town of Shirley network components. Internet access will be assigned. Passwords should be kept private and should be changed regularly. Attempts to access information on any Town of Shirley network components as any other user or to share a password may result in cancellation of user privileges. If a security problem is identified, notify the System Administrator; do not demonstrate the problem to other users.

Privacy

Users should not assume files stored on servers and hard drives of individual computers will always be private. Network administrators may review files and communications to maintain system integrity and insure that users are accessing the system responsibly.

Remote Access

Remote access defines the standards for connecting to the Town of Shirley network. It does not include use of the web-based mail client, Outlook Web Access (OWA). All employees have the ability to use OWA to access their mail from home or other locations.

Any remote access must use VPN or an encrypted remote access connection such as WebEx. Employee remote access to the network must be reviewed and approved by the Town Administrator. All employees by default will have account settings set to deny remote access.

Only upon written (email) approval by the Town Administrator will the employee account settings be changed to allow remote access.

The only exceptions to this policy are:

- Access may be given to outside technical support vendors and volunteers to provide support of town technology. Accounts will be approved on a case by case basis by the System Administrator.
- Remote access to the Accounting System is only allowed under the following conditions.
 1. Employees must use a Town issued laptop computer. Only Town owned computers may access the Accounting system.
 2. Employees may be allowed Administrative rights on the laptop on a case by case basis as approved by the System Administrator. Logon rights must be limited to User or Power User levels.
 3. Laptops must require a User ID and password to logon and resume from a sleep state or hibernation.
 4. Laptops must have a screen saver timeout set and require a password to resume.

Safeguarding Information

All employees are required to help safeguard information located on Town of Shirley computer systems. Employee obligations include, but are not limited to:

- Keeping usernames and passwords private.
- Storing files in home directories, on disks, or in shared folders on the network servers.
- Logging off the computer when away from the computer.

Social Networking

Recreational access and use of social networking sites such as Face book and MySpace on the town network is prohibited. Only business related social networking sites are permitted.

Software Security

Only members of the Technology Department (or persons designated by the System Administrator) are permitted to install software. All software purchased for use within the Town of Shirley computer network will be reviewed by the Technology Department to ensure network security and compatibility. The Technology Department will maintain a list of software and licenses.

Streaming Media

Recreational use of streaming media on the town network is prohibited.

Vandalism

Vandalism will result in cancellation of user privileges and disciplinary/legal action. Vandalism is defined as any malicious attempt to harm or destroy equipment, programs, and/or data of anyone connected to the network and/or Internet. This includes, but is not limited to, uploading, creating or transmitting computer viruses, hacking, theft and unauthorized intrusion.

Disclaimer

The Town of Shirley cannot be held accountable for the information that is retrieved via the network. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

The Town of Shirley will not be responsible for any damages individuals may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence or errors or omissions. Use of any information obtained is at employees own risk.

The Town of Shirley makes no warranties (expressed or implied) with respect to: the content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information; and any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.

The Town of Shirley reserves the right to change its policies and rules at any time in writing.

Consequences

The use of technology resources in the Town of Shirley is a privilege. Inappropriate or unethical use or failure to adhere to the guidelines may include, but is not restricted to, limitation or cancellation of user privileges, possible disciplinary action and/or appropriate legal action.

Please sign and return this sheet to the Town Administrator's Office.

The Town of Shirley reserves the right to change its policies and rules at any time in writing.

Consequences

The use of technology resources in the Town of Shirley is a privilege. Inappropriate or unethical use or failure to adhere to the guidelines may include, but is not restricted to, limitation or cancellation of user privileges, possible disciplinary action and/or appropriate legal action.

Acceptable Use Policy Application

User's Name: _____

(Please Print) (First) (Middle initial) (Last)

I have read, understand and will abide by the Town of Shirley Acceptable Use Policy. I understand certain violations of this policy may be unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary action and/or legal action may be taken. I understand that these guidelines apply whether I am using a town computer on the Town network or off-site.

User's Signature: _____

Date: _____