TOWN OF AYER
Electronic Communication Policy
Adopted by the Ayer Board of Selectmen on February 21, 2012

The Town of Ayer ("the Town") owns and maintains the following forms of electronic communication: internal and external electronic mail (email), voice mail, Intranet and Internet access ("Systems"). These Systems exist in order to further the Town's interests and support its operation and mission.

Some limited, non-business use is acceptable provided that the non-business use does not interfere with the Town's business needs or operation and does not violate state or federal law or any aspect of this policy.

All electronic communication systems are the property of the Town. All passwords, messages, attachments composed, sent, or received are the Town's property. Users should not consider any message or retained files to be private.

I. Legal Liability

This policy is in place to minimize the risk of legal liability to users and to the Town that might result from the use of our electronic communication and Systems.

Electronic mail is made available as a business communication tool and Town employees are obliged to use this tool in a responsible, effective and lawful manner. Although email might appear to be less formal than other written communication, it is subject to the same laws that apply to other forms of communication, such as those against defamation or those protecting intellectual or personal property rights. The Town's existing policies prohibiting sexual and other forms of harassment apply equally to the use of Town and other system components.

- If you should create or transmit any message or material with libelous, defamatory, harassing, offensive, racist or obscene content, you may incur personal liability for civil damages and/or be criminally prosecuted.

- If you violate client confidentiality by sharing or forwarding confidential information, other than on a need to know basis, and in accord with Town policy, you and/or the Town may be held liable for damages.

The use of Town or other Systems components in disregard or violation of the Electronic Communication Policy will result in personal liability to the user, and the Town will disassociate itself from the user as far as possible within the law.

II. Systems Monitoring

The Town has the right to, and will, monitor any and all employee, and/or town hall personnel electronic communications and usage on Town of Ayer computer equipment. Employees and town personnel must have no expectation of privacy in anything they create, store, send or receive on the Town's computer Systems.

Your electronic communications can be monitored without prior notification if the Town deems this necessary, in its sole discretion. All incoming and outgoing voice and messages and attachments are subject to access, review and disclosure in the ordinary course of administering the Systems, including communications that are password protected. Similarly, Internet web sites visited, private email systems and online email accounts (ie – yahoo mail, hotmail, etc.) and files downloaded will be evident to those employees responsible for administering that system. Additionally, the Town uses automated monitoring tools to continuously detect, block and/or quarantine files that may violate our policies or threaten the integrity of our Systems.

Employees responsible for administering the Systems are required to report any abuses of the Systems to the Town's administrators and managers. Indeed, certain illegal and unethical uses of the Town's Systems are required by law to be reported to the proper state authorities and law enforcement.

Violations of any part of the Electronic Communications Policy may result in disciplinary action, which, depending upon their severity or frequency may range from warning, suspension of privileges to possible discharge from employment with the Town of Ayer.

E-Mail created or received by an employee of a government unit may be a public record and offices must make email records available for public inspection. E-Mail messages are subject to public access through the Public Records Law. G.L. c. 66 § 10. A determination as to whether an email message is exempt from disclosure depends upon the content of the message. G. L. c. 4, § 7(26)(a-m)

All Town Employees and Special Town Employees (i.e. appointed and elected board/commission/committee members; volunteers; etc.) are required to use an official Town issued E-mail (in the form @ayer.ma.us) for all Town-related business. Using your personal E-Mail to conduct Town business puts your personal systems at risk for subpoena or discovery.

III. Activities Expressly Prohibited

The Town expressly prohibits the use of its Systems to:

- Commit a crime or violate any law, regulation or Town policy.
- Create, transmit, display or retain messages or materials that could reasonably be considered offensive, abusive, threatening, intimidating, hostile or harassing. Sending unwanted and/or offensive messages may constitute harassment if they are persistent enough to create an intimidating or hostile environment. Examples of such messages or materials include, but are not limited to:
    - Those with sexual content or requesting sexual favors.
    - Web sites containing: sexually explicit images or cartoons; racial or ethnic slurs; and/or comments that inappropriately concern any person's age, race, gender, sexual orientation, religion, national origin, ancestry or disability. For further explanation and examples, please refer to the Town's Sexual Harassment Policy and Harassment Policy (additional copies attached hereto).
- Use of the Systems to make an unauthorized attempt to enter into another employee's computer, or the computer of any third party (commonly referred to as "hacking"). Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.
- No employee shall send email under another employee's name without authorization and no employee shall change any portion of a previously sent email message without authorization.
- Employees are prohibited from storing information as outlined below on personal storage devices (PSD) such as portable hard drives, USB flash drives, phones, cameras or any other

PSD's unless authorized. Any such devices that contain personal information about employees, residents, vendors, businesses, or others must be pre-approved and encrypted to avoid unauthorized access to personal data. All staff members are obligated to follow the basic steps required to ensure safety of laptops, portable hard drives and other PSD's.
    - Do not leave portable devices unattended
    - Lock screen when PC powered on but not in use
    - Portable devices need to be password protected
    - Critical data needs to be Encrypted
    - Portable devices need to be secured when not in use
- Engage in computer games or gambling activity.
- Create or transmit "chain letters," or otherwise engage in "spam."
- Knowingly download or distribute pirated software or data.
- Conduct private or personal business, including any manner of non-Town related solicitation, whether commercial ventures, political, religious or other personal causes by any employee.
- Maliciously use or disrupt the Town's computers, networks, Internet services; or breach the Systems' security features; or misuse or damage the Town's computer equipment.
- Misuse computer passwords or accounts; or attempt to access unauthorized sites. Use of the Town's computers, networks and Internet services after such access has been denied or revoked; nor shall employees attempt to delete, erase or otherwise conceal any information stored on a Town's Systems that violates this Policy.
- Load, or download any software applications including (ie - themes, games, clocks, and weather), icons or screen savers of any kind to any computer unless previously authorized. Use of "instant messaging" functions, such as AOL Instant Messaging ("AIM"), MSN Messenger, Yahoo! Messenger, and the like are prohibited.
- Download or install Cellular phone software or comparable software without authorization and without coordinating with the IT Administrator for assistance to ensure appropriate security measures are in place.
- Allow any former employee, unauthorized persons, former elected persons to access the Town's Systems, and transmit or share in any form any Town materials or confidential materials to former employees, unauthorized persons, former elected persons without the express permission of town administrators.
- Violate copyright law and license agreements regarding software or publications accessed or downloaded from the Internet. The Town does not condone and will not defend violations of copyright laws and licenses.
- Open any attachments unless they are reasonably sure that the content is safe.
- Use any unauthorized computer (such as a home computer) to remotely access Town Systems.
- Engage in any activity that subjects the Systems to unwarranted exposure to viruses, worms or other potential damage.
- Attaching computers or other computer hardware that is not owned by the Town to the Town's Systems or Network.
- Employees are prohibited from sharing passwords and will be held accountable for all usage of the Systems under their passwords. No employee is to keep an unsecured written record of his or her passwords. If it proves necessary to keep a record of a password, then it must be kept in a locked controlled access area.
- Network and email passwords must be changed every 90 days. Passwords must be at least 8 characters in length and contain at least one UPPERCASE character, one lowercase character and one number.

Deleting an electronic mail message or other information does not necessarily mean the message cannot be retrieved from the Town's Systems. The Town routinely backs up system information and retains backup copies of all documents, including electronic mail messages produced and received on the Town's computer system. Electronic mail, once transmitted, can be printed, forwarded, and disclosed by the receiving party without the consent of the sender. Information within the Systems, including that stored in backup files, may be subject to disclosure in response to litigation discovery.

IV. Professionalism and Etiquette in Electronic Communications

Electronic mail should display care and professionalism, therefore, please adhere to the following practices:

- Write well-structured emails.
- Label every message with a short, descriptive subject, distinctive from other similar messages.
- Always use the spell check function before you send an email, in addition to visually scanning each message to detect errors not identified by spell check.
- Send only emails the content of which could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, marking the as confidential or using other means of communication.
- Mark an email as important only if it is justified.
- Do not indiscriminately copy all who may be on the sender's copy list when responding.
- Writing email in all Caps is considered Shouting

V. Questions

If you have any questions or comments about this Electronic Communications Policy, please contact the IT Systems Administrator or the Town Administrator. If you do not have any questions, the Town presumes that you understand and are aware of the rules and guidelines in the Electronic Communication Policy and will adhere to them.

Town of Ayer
Electronic Communication Policy

Declaration

I have read, understand and acknowledge receipt of the Electronic Communications Policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

_____ _____

Employee Signature Date

_____

Printed Name