

Town of Sangerville

POLICY ON COMPUTER USE AND E-MAIL/INTERNET ACCESS

OBJECTIVE:

To provide guidance on appropriate use of electronic mail, Internet, or other means of access to or use of resources made available to Town of Sangerville employees to communicate with each other, other governmental entities, companies and individuals for the benefit of the Town of Sangerville.

Use of the Internet by departmental employees is permitted and encouraged where such use is both suitable for business purposes and support the goals and objectives of the Department. In all cases, the Internet is to be used in a manner that is consistent with the Town's standards of conduct and as a part of the normal execution of an employee's job responsibilities.

POLICY:

The Town of Sangerville computer network, Electronic Mail System (e-mail) and Internet connection is designed to facilitate town business, and to provide for communications among employees and other business associates for messages or memoranda. Since no computer system is completely secure, the e-mail/Internet system is not intended to transmit sensitive materials, such as personnel decisions, and other similar information that may be more appropriately communicated by written memorandum or personal conversation.

The computer network, e-mail and Internet systems are Town of Sangerville property and intended for town business. Although some incidental use of the computer e-mail and Internet access for personal use is expected, it must be understood that such use is a privilege, which may be limited or removed if the privilege is abused or at any time, for any reason, at the discretion of the Town of Sangerville. Except for incidental personal use, no part of the system is to be used for employee personal gain or to support or advocate for non-business related activities or purposes. All data and electronic messages within this system are the property of the Town of Sangerville. As such, no computer files, or communications of any type through the Town's Electronic Mail System or Internet connection can be considered private. Electronic communications have been found to be public records and may be subject to the freedom of access laws, depending on their content. No use, or message, or communication within the system is private.

While you may have a confidential password, users should be aware that this does not mean that the system is for personal confidential communication, nor does it suggest that e-mail is the property right of the employee.

In addition, consistent with any confidential relationships or obligations with clients or program participants that may exist, Town of Sangerville reserves the right to authorize its directors, managers, and/or supervisors to review the contents of the employee's computer files, or e-mail/Internet communications whenever it may deem necessary for business or performance purposes. Employees may not intentionally intercept, eavesdrop, record, read, alter, or receive

other person's e-mail messages or computer files, without proper authorization. Passwords should be periodically changed to ensure security of the system. Users should not share their passwords with anyone else, other than as his or her managers may require. Employees may not provide or use alternative software to access the systems. Employees may not download or upload unauthorized software into the system.

The Internet provides the Town of Sangerville with significant access and dissemination of information to individuals outside of the organization. The use of the Internet for access and dissemination is intended to serve town business. Like all e-mail messages, Internet messages are capable of being forwarded without the express permission of the original author. Messages are also routinely passed through routers before they reach their final destination. A message is "touched" many times before it gets to its recipient, and the message author should be aware of this. Therefore, users must use caution in the transmission and dissemination of messages outside of the town, and must comply with all state and federal laws.

GENERAL PROHIBITIONS:

The Town's e-mail and Internet systems may be used only for lawful purposes. The transmission, distribution, or storage of any information, data, or material in violation of any applicable law, regulation or this policy is prohibited. Without limitation of the foregoing, it is prohibited to create, transmit, distribute or store any information, data, or material which:

- Is libelous, defamatory, hateful, or constitutes an illegal threat or abuse, or contains ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, age, disability, or religious beliefs.
- Is obscene or constitutes child pornography, contains sexually explicit images or messages, or may be construed as offensive, abusive, or threatening.
- Infringes any copyright, trademark, trade secret, or other intellectual property right.
- Is solicitation for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations except for incidental personal use.
- Is/or encourages, conduct that would constitute a criminal offense or give rise to civil liability.

GUIDELINES:

Employees are expected to abide by the generally accepted rules of computing and network etiquette. These include (but are not limited to) the following:

A. General Guidelines:

- Be polite.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- Do not reveal address or phone numbers of others. Providing both internal and your own personal address of phone number is personal choice but be aware that Internet transmissions can be monitored by others.
- Note that electronic mail (e-mail) is not private. Both internal and Internet transmissions can be easily intercepted by others and can be altered en route.
- Do not use computers or networks in such a way that you would disrupt their use by others. This includes being aware that you can create significant network traffic and consume scarce computing resources by your use of the Internet. Do not send large files needlessly.
- Use only services you have authorization to access.
- Always represent yourself as yourself – never someone else.

- Do not send un-encrypted town confidential or proprietary information over the Internet. If you are uncertain whether material is confidential or proprietary, consult your supervisor. If you need to utilize encryption, please contact the IT Liason who will provide directions.
- Material that would be considered inappropriate, offensive or disrespectful to others should not be accessed or stored.
- Respect copyrights and licenses.

B. Procedures:

1. Internet

- a. Access to the Internet is a tool provided by the Department to enhance their ability to perform their jobs by providing almost unlimited research opportunities.
- b. Generally employees will use the Internet for Job-related research only.
- c. Personal use of the Internet will be permitted only with permission of a supervisor provided such use does not interfere with or delay Department business. The supervisor will select the computer that the employee will operate for personal use.
- d. Employees may not download documents from the Internet unless the network real-time anti-virus program is running on the computer being used.
- e. No software may be downloaded from the Internet for installation on any Town computer without the approval of the Department Manager or his/her designee. The Department Manager will contact the IT Liaison for guidance. This is to ensure controls to ensure the integrity of each system remains intact.
- f. The employee requesting a software download from the internet will submit a request to the Department Manager or designee containing the name and manufacturer of the software and the reasons/uses for the installation request. The Department Manager will contact the IT Liaison for guidance. This is to ensure controls to ensure the integrity of each system remains intact.
- g. While using the Internet, employees shall not intentionally view or download electronic images that contain nudity, pornography, child pornography or other images, words or language that are sexually explicit of a sexually suggestive nature unless part of an approved criminal investigation.
- h. If any of the aforementioned websites are unintentionally accessed, the employee shall notify his/her immediate supervisor explaining the circumstances surrounding the access.

2. E-Mail

- a. The use of electronic mail by Department personnel is encouraged as a method of conducting business only.
- b. The electronic mail system and all messages created therein are the property of the Department and intended solely for the Department's business purposes.
- c. Authorized uses of e-mail include:
 - i. To facilitate performance of job functions.
 - ii. To facilitate the communication of information in a timely fashion.
 - iii. To coordinate resources, location and individuals for agency and inter-agency meetings.
 - iv. Personal use may be approved by the Department Manager.
- d. Unauthorized uses of e-mail include but are not limited to:
 - i. Personal use not approved by the Department Manager, including access of non-municipal, personal e-mail accounts from any Town Departments or Town equipment.
 - ii. The transmission of confidential information.
 - iii. Use in violation of any Federal, State, or local law.
 - iv. Communications containing threats or harassing or intimidating statements.
 - v. Communications containing defaming, slanderous or libelous statements.
 - vi. Obscene, offensive or suggestive messages or graphical images.
 - vii. Racial, religious, ethnic or sexual slurs.

- viii. Possession, storage or transmission of messages containing nudity, pornography, child pornography or other images, words or language that are sexually explicit or sexually suggestive nature.
- ix. Commercial activities or solicitations.
- x. Misrepresenting one's identity while using e-mail.
- xi. Intercepting, disrupting or altering electronic communications.
- xii. Sending copies of documents in violation of copyright laws.

C. Security Responsibilities:

- If you identify a security problem, notify the Department Manager immediately.
- Do not show or identify a security problem to others.
- Do not reveal your account password or allow another person to use your account. Only authorized personnel will have access to your account password.
- Do not use another individual's account.
- Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

D. Vandalism/Harassment:

- Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet or other networks. This includes, but is not limited to, creating and/or knowingly uploading computer viruses.
- Vandalism and/or harassment will result in the cancellation of the offending user's account and/or further disciplinary action.
- Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes, but is not limited to, the sending of unwanted e-mail.

E. No Expectations of Privacy:

- Employees shall have no expectations of privacy when using Department authorized or provided communications or computer systems.
- All Department computers, including all hardware, software, files, data, documents, caches and electronic mail are subject to random and unannounced inspections by the Department Manager.
- The Town of Sangerville reserves the right, when not in conflict with any law, to inspect, monitor, remove and read electronic messages, including computer files, caches, data, electronic mail, graphics or digital photographs, to decipher encrypted files, text and messages and to remove or inspect any software, especially software installed or altered without authorizations.

F. General Information:

- The Town prohibits any unauthorized copying of license software as a violation of copyright laws.
- Games may not be loaded.
- Hardware items are not to be loaded or removed unless authorized by the Department Manager.
- Any violation of this policy will result in disciplinary action.

Generally, messages are intended to be temporary communications that are non-vital and may be discarded routinely. However, depending on the content of the message, it may be considered a more formal record and should be retained pursuant to a department's record retention schedule. As such, these messages are similar to printed communication and should be written with the same care. Each department's retention schedule for other forms of communication should apply to electronic communications as well.

Employees should be aware that when they have deleted a message from their workstation mailbox, it might not have been deleted from the centralized systems. The message may be residing in the recipient's mailbox or be forwarded to other recipients. Furthermore, the message may be stored on the systems backups for an indefinite period. Employees should delete personal messages as soon as possible after reading. An accumulation of files will degrade system performance and response times. This policy applies to all employees, contractors, part-time employees, volunteers, and other individuals who are provided access to the Town's system. Third parties should only be provided access to the system as necessary for their business purpose with the Town and only if they abide by all applicable rules.

Employees who leave employment with the Town of Sangerville have no right to the contents of their e-mail messages and are not allowed access to the e-mail system. Supervisors or management may access an employee's e-mail if employees are on leave of absence, vacation, or are transferred from one department to another department and it is necessary for the Town's business purposes.

The misuse of the Internet or e-mail privileges may be considered sufficient cause for discipline in accordance with the Personnel Policies and Procedures, and/or other applicable rules or laws. In addition, in the event of suspected, alleged or actual illegal activity, the Town may notify or cooperate with applicable law enforcement authorities for potential civil or criminal investigation or prosecution.

Acknowledged

Date given to Staff by Department Manager: _____

Department Manager Signature: _____

Acknowledgement of Receipt and Understanding of Policy:

Each Employee shall read and sign the acknowledgement which will then be placed into his or her personnel file in the Town Manager's office.

Employee

Date