Town of Guilderland

Technology Policy & Procedure

Functions and duties of the office:

1. To aid with official town planning and coordinating for the advancement of technology to improve town government efficiency and effectiveness, and perform all necessary and appropriate services required to fulfill these duties;
2. To advise and assist the town departments in developing policies, plans and programs for improving the town-wide coordination, administration, security, confidentiality, program effectiveness, acquisition and deployment of technology;
3. To perform technology reviews and make recommendations for improving management and program effectiveness pertaining to technology;
4. To review and coordinate the purchase of technology by town departments. Where applicable, such review shall include but not be limited to: assessing consistency with the strategic long-term technology plan; the safeguarding of information privacy; security of confidential records; and proper dissemination of public information;
5. To establish, oversee, manage, coordinate and facilitate the planning, design and implementation of the town's technology networks;
6. To undertake research, studies and analyses, with respect to technology;
7. To facilitate and coordinate the improvement of program delivery services through technology with and among other departments of the town;
8. To establish technology policies, including but not limited to preferred technology standards and security, including town-wide policies, standards, programs, and services relating to the security of town department networks;
9. To adopt, amend, or rescind rules and regulations necessary or convenient to the performance of the functions and duties of the office;
10. To complete a comprehensive study of existing town information resource technology infrastructure to the extent that the information is available. Such study shall include, but not be limited to, inventories of:

    (a) town operations' computer hardware and software;

    (b) major physical infrastructures supporting existing operations, including power, air conditioning, space and other environmental needs;

    (c) the telecommunications and other networks supporting existing operations;

    (d) personnel associated with existing operations and management;

    (e) expected retirement schedule of existing computer hardware and software and replacement costs; and

    (f) data processing consulting and contracting services utilized.

    Such study shall be completed and submitted to the town supervisor on a yearly basis.

    10-a. To develop:

    (a) a methodology to ascertain how much the town spends on technology goods and services;

    (b) a process to update the computer hardware and software inventory periodically;

    (c) a methodology to determine the expected life-cycle of town operations' computer hardware and software which shall include the total cost of ownership; and

    (d) formal disaster recovery plans for the town data center and network.

10-b. To request and shall receive from any department, any information and resources necessary to carry out the responsibilities and provisions set forth in subdivisions ten and ten-a of this section.

11. To conduct selective evaluations of technology activities in town departments; and
12. To perform such acts, directly or by other means, as are necessary or convenient to carry out the office's functions and duties.
13. To enter into contracts with any person, firm, corporation, not-for-profit corporation, or governmental entity as directed.
14. To provide for the protection of the town government's cyber security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the town.
15. To maintain, in electronic or paper formats, maps, geographic images, geographic data and metadata.

Responsibility to respond to the freedom of information law for certain data. Where the office receives a request for data which is in the possession of the office because it administers, operates or manages a townwide technology program, the office will transmit, within five days, a copy of the transmittal to the requester.

Severability. The provisions of this article shall be severable and if any portion thereof or the applicability thereof to any person or circumstances shall be held to be invalid, the remainder of this article and the application thereof shall not be affected thereby.

Security

Data protection

Safeguarding electronic data is paramount for town owned computer equipment. All computer devices will have licensed virus and malware protection software. Disabling or removing said protection software is not allowed. Virus protection must be active and licensed on all town computers. There will be active and daily administrative monitoring of all town PC devices and virus definition updates.
Administrative access to the local PCs and Servers is not allowed for the security and safeguarding of town computer equipment.
Software may not be downloaded and/or installed on town computers.
Personal devices may not attach to the town network for the security of the town equipment and data. However, wireless devices may be set up on a segregated SSID on a separate virtual network for access to the internet only.
Remote access to town computers and servers from home/personal devices is not allowed for the security and safeguarding of those devices.

Password security

Users are responsible for safeguarding their passwords for access to the computer system. ***Individual passwords should not be printed, stored online, or given to others.*** Users are responsible for all transactions made using their passwords; accordingly, care should be taken to protect your password from detection by others, and your password should be changed periodically. It is strongly suggested that all users log off the network when away from their desks for an extended time period. Users may not access the computer system with another user's password. When it is necessary to have several people working on a common document, you should use shared folders (where the document can be accessed by others) in order to preserve password integrity.

Disposing/sanitizing computer equipment

Because of sensitive materials and information, computers will not be thrown away, donated or sold. All computer equipment – with data storage capability – must be recycled through an NYS EERA Covered Electronic Equipment recycling company. Said company will also be authorized NYS Data Destruction contractor. Certificates of recycling will be kept on file along with required NAID certificate of hard drive data destruction.

Employee Acceptable Use Policy

Acceptable computer use

-Administrative access to the local PCs and Servers is not allowed for the security and safeguarding of town computer equipment.

-Software may not be downloaded and/or installed on town computers. To prevent the downloading of computer viruses, malware or programmatic errors and conflicts with installed software, no employee may download software from the Internet without prior authorization from the IT department. Any and all software that is downloaded or installed must be licensed and registered to the Town. No unauthorized software of any kind should be added to the Town's system, including screensavers or games.

-Personal devices may not attach to the town network for the security of the town equipment and data. However, wireless devices may be set up on a segregated SSID on a separate virtual network for access to the internet only.

-Remote access to town computers and servers from home/personal devices is not allowed for the security and safeguarding of those devices.

-Disabling or removing virus/malware protection software is not allowed.

-Users are responsible for safeguarding their passwords for access to the computer system. ***Individual passwords should not be printed, stored online, or given to others.*** Users are responsible for all transactions made using their passwords; accordingly, care should be taken to protect your password from detection by others, and your password should be changed periodically. It is strongly suggested that all users log off the network when away from their desks for an extended time period. Users may not access the computer system with another user's password. When it is necessary to have several people working on a common document, you should use shared folders (where the document can be accessed by others) in order to preserve password integrity.

Acceptable email use

Section 1 - Purpose and Goals

E-mail is one of the Town of Guilderland's core communication methods. The purpose of this policy is to ensure that the Town's e-mail system is used to support Town business functions. This policy advises staff and management of their responsibilities with regard to the use of e-mail and provides guidance in managing information communicated by this method.

Section 2 - Access to E-mail Services

E-mail services are provided to all PC users connected to a Local Area Network.

Section 3 - Use of E-mail

E-mail services, like other means of communication, are to be used to support Town business. Staff may use e-mail to communicate outside of the Town when such communications are related to legitimate business activities and are within their job assignments or responsibilities. Staff may not use e-mail for illegal, disruptive, unethical or unprofessional activities or for personal gain, or for any purpose that would jeopardize the legitimate interests of the Town.

Section 4 - Privacy and Access

E-mail messages are not personal and private. The Town will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail. However, Network managers and technical staff may access an employee's email:

- for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time) ;
- to diagnose and resolve technical problems involving system hardware, software or communications; and/or
- to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an appropriate investigation.

A staff member is prohibited from accessing another user's e-mail without his or her permission.

E-mail messages sent or received in conjunction with Town business may:

- be releasable to the public under the Freedom of Information Law;
- require special measure to comply with the Personal Privacy Protection Law.

All e-mail messages, including personal communications, may be subject to discovery proceedings in the legal actions.

Section 5 - Security

E-mail security is the responsibility of e-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of the account by unauthorized individuals.

Section 6 - Management and retention of e-mail communications:

A. *Applicable to all e-mail messages and attachments*: Since e-mail is a communications system, messages should not be retained for extended periods of time. Users should remove all e-mail communications in a timely fashion. If a user needs to retain information in an e-mail message for an extended period of time, he or she should transfer it from the e-mail system to an appropriate electronic or other filing system. The Town is authorized to remove any information retained in an e-mail system that is more than 60 days old. Users will be notified prior to this action to give them the opportunity to save any message they need to retain.

B. *Applicable to records communicated via e-mail*. E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements under the Arts and Cultural Affairs Law and specific program requirements.

Examples of message sent by e-mail that typically are records include:

- policies and directives,
- correspondence or memoranda related to official business,
- work schedule and assignments,
- agendas and minutes of meetings,
- drafts of documents that are circulated for comment or approval,
- any document that initiates, authorizes or completes a business transaction, final reports or recommendations.

Some examples of messages that typically do not constitute records are:

- personal messages and announcements,
- copies or extracts of documents distributed for convenience or reference,
- phone message slips,
- announcements of social events.

C. *Record Retention:* Records communicated using e-mail need to be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system outside the e-mail system. Records communicated via e-mail will be disposed of within the record

keeping system in which they have been filed in accordance with a Records Disposition Authorization (RDA) approved by Records Management Officer. Department heads should consult with the Records Management Officer concerning RDAs applicable to their department's records.

Users should:

- dispose of copies of records in e-mail after they have been filed in a record keeping system;
- delete records of transitory or little value that are not normally retained in record keeping systems as evidence of town activity.

Section 7 - Roles and Responsibilities

The Town will insure that policies are implemented by Department Heads. Department Heads will develop and/or publicize record keeping practices in their area of responsibility including the routing, format and filing of records communicated via e-mail. They will train staff in appropriate use and be responsible for ensuring the security of physical devices, passwords and proper usage.

The Town Clerk's Office shall be responsible for backup and disaster recovery.

All e-mail users should:

- be courteous and follow accepted standards of etiquette.
- protect other's privacy and confidentiality.
- consider organizational access before sending, filing or destroying e-mail messages.
- protect their passwords.
- remove personal messages, transient records and reference copies in a timely manner.
- comply with Town policies, procedures and standards.

Section 8 - Policy Review and Update

The Town will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be forwarded to the Town Supervisor.

Acceptable internet use

This policy is to ensure that Internet facilities are to support Town business functions. This policy advises staff and management of their responsibilities with regard to the use of the Internet and provides guidance in managing information obtained or communicated by this method.

The connection to the global Internet and the World Wide Web exists exclusively to facilitate the official work of the Town of Guilderland. The Internet facilities and services will contribute broadly to the missions of the Town and it's various programs.

Section 1 - Access to the Internet

Access to the Internet is provided primarily through the Town's existing Local Area Network (LAN) structure, and to a lesser degree, through connections utilizing third party providers.

These Internet facilities are provided only for employees and persons legitimately affiliated with the Town for the efficient exchange of information and for the completion of assigned responsibilities consistent with the Town's statutory purposes.

It is the responsibility of each Department Head to determine which staff members should be provided with this access.

Section 2 - Principles of Acceptable Use

The use of Internet access facilities by any employee or any other person authorized by the Town must be consistent with this Acceptable Use Policy and with security policies.

Staff may use the Internet only when such use is related to legitimate business activities and is used to complete job assignments and official responsibilities. Specifically, users of the Internet are required to:

- respect the privacy of others. Users shall not intentionally seek information on, obtain copies of, or modify files or data belonging to other users, unless explicit permission to do so has been obtained;
- respect the legal protection provided to programs and data by copyright and license;

- protect data from unauthorized use or disclosure as required by state and federal laws and Town regulations;
- respect the integrity of computing systems. Users shall not use or develop programs that harass others or infiltrate a computer or computing system or damage or alter the software components of a computer or computing system;
- comply with other Town policies on computer, software and e-mail use. Specifically, no software obtained from any source, including the Internet, shall be installed or used on any computer or computing system of the Town without the prior authorization of the Town Supervisor;
- safeguard their accounts and passwords. Any user changes of passwords must follow published guidelines for good passwords. Accounts and passwords shall not be shared. Users shall report any observances of attempted security violations.

Section 3 - Unacceptable Use

It is not acceptable to use Town of Guilderland Internet access facilities for:

- activities unrelated to the Town's mission;
- activities unrelated to official assignments and/or job responsibilities;
- any illegal purpose or activities;
- transmitting threatening, obscene or harassing materials or correspondence;
- unauthorized distribution of network users of Town of Guilderland data or information;
- interference with or disruption of network users, services or equipment;
- private purposes such as marketing or business transactions;
- solicitation for religious and political causes;
- unauthorized not-for-profit business activities;
- private advertising of products or services;
- any activity meant to foster personal gain; or
- any other purpose that would jeopardize the legitimate interest of the Town.

Section 4 - Privacy

Pursuant to the Electronic Communications Privacy Act of 1986 (18 U.S.C. 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 full access to all mail and user access requests. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

The Town reserves the right to log network use and monitor file server space utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.

While there will not be routine monitoring of the content of electronic messages and communications, there will be regular review of usage logs to assure efficient performance and appropriate use. Records of Internet use and user activity will be maintained and periodically distributed to program managers for review.

Section 5 - Rights of the Town

The Town reserves the right to remove a user account from the network or restrict access to the Internet.

The Town will not be responsible for any damages, including the loss of data resulting from delays, non-deliveries or service interruptions caused by negligence, errors or omissions. The use of any information obtained is at the user's risk. The Town makes no warranties, either express or implied, with regard to software obtained from this system.

The Town reserves the right to change its policies and rules at any time. The Town makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:

- the content of any advice or information received by a user or any costs or charges incurred as a result of seeking or accepting such advice;
- any costs, liabilities or damages caused by the way the user chooses to use Internet access; or
- any consequences of service interruptions or changes, even if they arise from circumstances under the control of the Town. The Town's Internet services are provided on an as is, as available basis.

Section 6 - Enforcement and Violations

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Town's Internet facilities and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of unacceptable uses should be directed to the Town Supervisor. Other questions about appropriate use should be directed to your supervisor.

The Town will investigate allegations of violations of the Internet Acceptable Use Policy on a case-by-case basis. Violations of this policy which are not promptly remedied will result in termination of Internet access services for the person(s) at fault, and referral for other administrative actions as appropriate.

VIOLATIONS

All employees are required to acknowledge receipt of the Town's Computer, E-mail and Internet Use Policy, and to agree to follow the established guidelines. The guidelines are intended to clearly inform all users of appropriate uses of the Town's computer network, and to protect the integrity of the system's security, thereby minimizing downtime of the system. The policy is also intended to protect all employees from potentially being exposed to offensive material and behaviors.

Any employee who violates these rules or otherwise abuses the job-required use of the Town's E-mail or Internet system will be subject to corrective action, up to and including termination. If necessary, the Town also reserves the right to advise appropriate officials of any illegal activities.

Internet security and privacy policy

1. The Town of Guilderland will not disseminate any information, including personal contact information, the town website may collect with respect to the user to any person, firm, partnership, corporation, LLC or any other entity, including internal staff;
2. There are no circumstances under which information, including personal contact information, collected may be disclosed;
3. The information collected will be retained by the town indefinitely unless requested to remove such contact information;
4. The website has specific instructions for subscription procedures to both add contact information and remove contact information;
5. the means by which contact information is collected is user initiated and the collection occurs actively;
6. The collection of information is voluntary;
7. The town protects the confidentiality and integrity of the information through use of secure encryption of the website contents and firewall protection, both in-house and with regarding to the hosting vendor;
8. The Town of Guilderland will adopt an internet privacy policy and post such policy on its website;
9. The internet privacy policy shall be made available at no charge to other public and private entities;

Exceptions. Town may disclose personal information if the collection or disclosure is:

1. made pursuant to a court order or by law;

The Town of Guilderland's policy is to respect and protect the privacy of its website users. However, if you choose to provide us with personal information, such as an e-mail to Town staff or by filling out a form with your personal information and submitting it to us through e-mail, we use that information to respond to your message and to help us get the information you have requested. We do not collect personal information for any other purpose other than to respond to you and we do not create individual profiles. However, information we receive may be considered public information, which is subject to disclosure under New York State law.

Notification

Person without valid authorization has acquired private information

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

1. "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the town. Good faith acquisition of personal information by an employee or agent of the town for the purposes of town use is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.
2. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the town may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

1. The town, with regards to any town owned or licensed computerized data that includes private information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The town shall consult with the state office of cyber security and critical infrastructure coordination to determine the scope of the breach and restoration measures.
2. The town, with regards to maintaining computerized data that includes private information which the town does not own, shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.
3. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
4. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification

is kept by the town employee or agent who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the town who notifies affected persons; or

(d) Substitute notice, if town demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or town does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when town has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on town's web site page; and

(3) notification to major statewide media.

5. Regardless of the method by which notice is provided, such notice shall include contact information for the town and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.
6. (a) In the event that any New York residents are to be notified, the town shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. (b) In the event that more than five thousand New York residents are to be notified at one time, the town shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.