TOWN OF GRAFTON
Grafton Memorial Municipal Center
30 Providence Road
Grafton, Massachusetts 01519

Computer Information and Resources Policy

POLICY:
The purpose of this Policy is to provide guidance to all Users concerning their responsibility and obligations with respect to the information generated and communicated by the Town's Computer Resources; and to ensure that Computer hardware/software Resources and associated information are used responsibly, ethically, and lawfully. It is the Town's policy that all computer resources should be used primarily for effective management and communication of business information.

Scope: All employees, permanent, per diem, temporary, independent contractors, consultants, temporary workers, interns, elected officials, appointed officials, and other persons or entities who use our Town's computer resources.

Description: All users must comply with the provisions of this Policy and must refrain from using the Town's Computer Resources for personal gain or in a manner that creates a conflict of interest or violates the law.

Definitions:

A. Town - The Town of Grafton affiliates and successors.

B. Computer Resources - The Town's entire interconnected computer system, including, but not limited to, mainframe computers, midrange computers, file servers, application servers, communication servers, email servers, internet servers, intranet servers, web servers, desktop and laptop computers, operating system software, application program software, data files, data storage, WiFi networks, and all internal and external communication and support systems which are directly or indirectly connected to the computer system, including cell phones and other mobile internet devices.

C. Departments - Groups of Users assigned to manage a set of similar business processes.

D. Information - The digital intelligence created by, stored within, displayed on, and printed from our Computer Resources.

E. Malware- Malicious code or a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or integrity of the victim's data.

Generally, malicious code is designed to perform these nefarious functions without the system's user knowledge.

F. Shared Computer Resources - Computer resources specifically designed to facilitate the communication of, and collaboration around, information. Examples of shared computer resources are Town email, intranet services, and shared directories.

G. Users - All employees, independent contractors, consultants, temporary workers, elected officials, appointed officials, and other persons or entities who use our Town's Computer Resources.

Town Property

A. Access to the Town's Computer Resources is provided to Users to assist in job performance.

B. The resources are not intended for private use and the users should not have any expectations of privacy relative to any Information he/she creates, stores, sends, or receives through the Town's Computer Resources.

C. Town issued mobile resources such as iPads and other tablets are required to be linked to the Town Mobile Device Management software.

D. Information should not be considered either confidential or secure unless the User takes appropriate steps to make it so.

E. The individual User has the responsibility to designate information that is confidential as such, and control access to any information that is considered confidential in the business.

F. Users should be aware that Information which has been sent to others can be forwarded by recipients to other Users and outside parties, printed, and ultimately read by anyone who sees the printed message; inadvertently routed to a User other than the intended recipient; and potentially accessed by others if PCs are unattended.

Right to Monitor

Although it will not be the policy of the Town to monitor user information in general, the Town reserves the right and will do so for the performance of operation, maintenance, auditing, security, legal, and investigative functions. The information gained in this way may be used in disciplinary or criminal proceedings. Employees acknowledge and understand they have no right to privacy in regard to the use of the Town's Computer Resources. Monitoring may be undertaken for the following reasons:

A. To ensure compliance with relevant regulations and Town of Grafton standards (including the policy and these guidelines)

B. To prevent and detect criminal activity

C. To investigate/detect unauthorized use of Computer Resources

D. To respond when Users have logged a request for e-mail or Internet assistance

E. To ensure efficient system performance

F. To establish facts, e.g., whether personal use is interfering with Computer Resources and/or employee's performance

G. To ensure continued business performance in the event of an employee's absence

The decision to monitor will be made by the Town Administrator, in consultation with the Human Resource's Director, and Town Counsel.

Responsibilities

A. Town Administrator or designated Town provider is responsible for:

1. The design, installation, operation, and maintenance of town computer resources.
2. The security, integrity, storage, communication, delivery, and presentation of town information, the establishment of retention periods for Shared Computer Resources Information, such as email (refer to Section XI).
3. The purchase and financial maintenance of periodic replacement of Town PC Computer Resources

B. Town Departments are responsible for:

1. The recommendations for purchase of PC Computer Resources when additional resources are needed above periodic replacement.
2. The ownership, use, maintenance, classification of sensitivity and access to their specific Town department information.
3. Ensuring that employee use of computer resources has been properly authorized and is properly monitored.

C. Each User is responsible for:

1. Reading and understanding this Policy and ensuring that he/she abides by it.
2. Periodically reviewing all of his/her information to determine what needs to be archived, what needs to be backed up, what needs to be copied, what needs to be printed, and what needs to be deleted.

3. Using Shared Computer Resources (such as email) effectively. Care should be taken in addressing messages and in standardizing file formats for attachments. Large files, such as spread sheets, graphics, and CAD drawing files, should be stored using the appropriate type of computer resources.
4. Ensuring the accuracy and completeness of data that he/she distributes electronically.
5. Accessing information only as authorized in the performance of his/her job function.
6. Processing information only under the authorization of his/her ID and passwords.
7. Understanding that the Town will not be liable for any disclosure of personal Information of others and the user by the User. (whose personal info)
8. Respecting the rights of other Users; and
9. Informing the Town Administrator of any abuses of this policy.

Prohibited Activities

The following activities are strictly prohibited:

A. Sending, receiving, downloading, displaying, printing or otherwise disseminating information that is sexually explicit, profane, obscene, harassing, threatening, intimidating, fraudulent, racially offensive or discriminatory, defamatory, or otherwise unlawful. The Town reserves the right to block any internet sites including but not limited to those that contain information that fall within these categories as well as weapons, gambling, drugs, hacking and remote proxy type sites.

B. Entering, examining, using, transferring, or tampering with information of others unless appropriately authorized pursuant to this policy.

C. Installing, applying, or using any software that has the capability of compromising system security; or interfering with the work of other Users. The installation of any new software program or application should be authorized by the Town Administrator or the Town's IT Support Services vendor.

D. Connecting non-Town computers or computer peripherals into the Town of Grafton Network.

E. Disseminating or storing commercial or personal advertisements, solicitations, promotions, destructive programs (viruses), non-authorized political information, or any other unauthorized information.

F. Wasting or staining computer resources, including, but not limited to, sending mass mailings or chain letters, spending excessive amounts of

time on the internet, viewing audio or video intensive websites unrelated to business activities, playing computer games, engaging in on-line chat groups, printing multiple copies of documents or otherwise creating unnecessary Computer Resource traffic.

G. Without prior authorization from the Town Administrator, copying software for use on home computers, providing copies of software to any third parties, including independent contractors or consultants; installing operating system software on any Town workstation or server; downloading any operating system software from the internet or other online service to any Town workstation or server; modifying, revising, transforming, recasting or adapting any licensed software; or reverse-engineering, disassembling, or de-compiling any licensed software.

H. Violating any license agreement, copyright, or trademark law; or

I. Violating any state, federal, or international law.

Users encountering or receiving illegal or inappropriate materials, as described above or Users who become aware of any misuse of Computer Resources or Town Information should immediately report the incident to their supervisor, who, in turn, should notify either the Town Administrator or the Select Board.

Security

Responsibility for Computer Resources and information security must be shared.
The Town Administrator or designee is responsible for the following:

A. Designing, maintaining, installing, and updating Computer Resources with appropriate security, especially at interface points between Town Computer Resources and the computer resources of others.

B. Rapid identification, correction, and documentation of security breaches that do occur.

C. With the Town Counsel, investigation of the nature and consequences of any security breach which is more than minor in nature.

D. Policy distribution and sign off for all existing employees and any new employee upon hire, or when a policy change is adopted.

Town Departments are responsible for specifying the nature of their Computer Resources and information security needs to the Town Administrator for any need not considered routine in nature.

Employee Security Responsibilities

A. Employees are required to lock their terminal when away from their desk to prevent non-Users from accessing the Towns Computer Resources without authorization.

B. Safeguarding identification code(s) and password(s), using them only as authorized. Keeping passwords private. If an employee shares their access code and/or password disciplinary action may be taken (codes should be changed immediately)

C. Immediately changing identification code(s) or password(s) if you know or suspect that they have been compromised and then notifying your supervisor. Incidents should be reported to the Town Administrator or the Town's IT Support Services vendor.

D. Refraining from copying information belonging to another User without first obtaining permission from the owner of that information. Refraining from connecting directly to another User's or non-User's computer resources except through the Town's Computer Resources.

E. Peer to peer type software and the unauthorized use of remote-control software is prohibited.

F. Care should be taken while administering shared directories to store only information that should be shared and to limit directory access to only those individuals who should have access to that information.

G. Physically securing any Flash drive, portable hard drive, or other portable data device with sensitive information. Desktop PCs are only as secure as your office area. Being aware that messages stored on Shared Computer Resources (like email) are customarily backed up and archived in a media which can be later read, rewritten, or resent by others.

H. Accessing the internet through a PC attached to the Town's Computer Resources must be only through the Town maintained internet firewall. Accessing the internet directly, by modem through an external ISP or otherwise, is strictly prohibited.

Viruses & Malware

Viruses are a special class of security breach which can rapidly cause substantial damage to Computer Resources and Town information. Viruses and malware can be introduced into our Computer Resources at any point of interface between our resources and the computer resources of others. The two most common points of troublesome interface are the loading of "foreign" USB drives, CDs, and other portable drives onto our PCs and downloading files from email or internet sources into our Computer Resources.

1. Each user is responsible for taking reasonable precautions to ensure that he/she does not introduce viruses into the Town's Computer Resources.

2. Users should make every effort to obtain CDs and foreign email and internet files from known and reputable sources.

3. If User have doubts about the integrity of foreign portable drivers and CDs, they should contact the TA or designee *before* loading these devices into their PC. Contact them for instructions *before* introducing any suspected file into our Computer Resources.

4. As a further line of virus and malware defense, the town maintains updated virus scanning systems on its Computer Resources.

5. Users receiving messages on their PCs indicating the presence of a virus should immediately contact the Town Administrator or the Town's IT Support Services vendor. Scanning systems scan the i email and most attachments that are received by the Town mail system; therefore, the Town email system is the only authorized way of receiving and sending emails through the Town's Computer Resources.

6. All use of external main services (e.g., Gmail, Hotmail, and others) is prohibited.

Shared Computer Resources

Shared Computer Resources are specifically designed to facilitate the rapid and wide communication of, and effective group collaboration around information.

Shared Computer Resources can and should be used to facilitate rapid communication of, and collaboration around, any information Users that would be willing to commit to paper. However, it is not appropriate to use Shared Computer Resources for all business uses. In general, it is not advisable to put into electronic form any information you would not want to appear on paper.

Electronic documents are fully discoverable under Public Record laws. information stored anywhere may come to light under regulatory or legal subpoena, including information stored by the Town's Shared Computer Resources for any reason. Therefore, Shared Computer Resources should not be used when:

1. Dealing with extremely confidential information.

2. Handling situations where misunderstandings or confusion is known to or may exist; or

3. Dealing with documents of record. These should be printed and distributed as paper copies. Examples of these are legal documents and documents based on pre-printed forms.

4. Personal use violations also put the town at risk for outside subpoenas not related to town business.

5. In addition, care should be used when:

    A. Dealing with privileged or confidential information.

    B. Handling situations where immediate information communication to the recipient is critical. As an example, the sending of an email should not assume the recipients check their mailboxes on any particular schedule or frequency. In addition, there are variations in message delivery times across internal and external computer resources that may affect how quickly a message becomes available to the recipient.

    C. Considering message storage with reference to Town email, Users should be aware that the Town currently adheres to the following message retention schedule, largely independent of User initiated message deletions:

        1. Inbox- 90 days
        2. Sent items- 90 days
        3. Deleted items- 30 days
        4. Calendar items- 365 days

Wireless Communication Points

Wireless Communication Points may be provided in certain public areas for the sole purpose of gaining access to the internet. All other internet access for non-Town PCs is forbidden. Suspected or known violations of this Policy should be reported immediately to the Town Administrator or the Select Board. Alleged violations will be immediately investigated and appropriate disciplinary action, up to and including termination, will be taken. Violations may also result in revocation of Computer Resources privileges, referral to law enforcement agencies, or other legal action.

Approved By: Select Board Date: 9/21/2021

Peter Carlson, Chair

Colleen Roy, Vice Chair

Mathew Often, Clerk

Doreen DeFazio, Member

Raymond Mead, Member

ATTACHMENT A
TOWN OF GRAFTON
EMPLOYEE CONFIRMATION OF RECEIPT

I hereby certify that I was given a copy of the Computer Information and Resources Policy, and have been given an opportunity to ask questions of my superior about the content of the policy. I certify that I have read and understand the contents of this policy.

_____
Employee's name

_____
Department

_____
Employee's Signature

_____
Date

Revised September 24, 2021