TOWN OF HOPKINTON

HUMAN RESOURCES DEPARTMENT

Town Hall
18 Main Street Hopkinton, Massachusetts 01748

Maryrose DeGroot
Human Resources Director

Telephone: 508-497-3407 Fax: 508-497-9702
e-mail: Maryrose@hopkinton.org

Town of Hopkinton Technology Policy

Introduction: The Town of Hopkinton "The Town" provides access to technology in order to support and enhance the delivery of services, business processes, and facilitate appropriate communication. The Town believes that the resources and efficiencies available through the use of technology are of significant value in accomplishing these objectives, and expects that all such use shall be consistent with these objectives. At the same time, the Town appreciates that the wealth and diversity of available resources requires that reasonable controls be established for the lawful, efficient and appropriate use of this technology.

These controls have been developed in the form of implementing regulations, noted in this policy. These regulations shall be reviewed and updated as necessary and appropriate by the IT Officer. The Director of Human Resources shall serve as the custodian of these regulations and ensure their timely distribution as necessary. All new staff members shall be provided with a copy of this policy at the time of hire and before beginning work.

B1. Technology, In General:

Information Technology is defined as:

- Computers (including servers, workstations, laptops and handheld devices)
- Computer-related hardware (including printers, scanners, special devices)
- Software (including networks and the Internet)
- Telephones, Modems & Handheld devices
- Town Information Technology infrastructure includes all networks, computers, modems, hubs, software and data.

The Information/Technology (IT) Officer for the Town of Hopkinton is the Town Manager or his or her designee.

The Town will ensure the security, integrity and performance of all information technology hardware, software, data, and transaction processes on Town property.

B2. Use of Technology:

The acceptable use of information technology is an important concern for all employees and elected and appointed officials of the Town. Acceptable use rules are as follows:

- All unapproved software and executable programs are strictly prohibited.

- Technology should be used primarily for official Town purposes related to the conduct of Town government, to accomplish job responsibilities more effectively. Other uses, such as commercial or political use are expressly prohibited.

- Incidental personal use of technology such as Town e-mail is permitted but, like all e-mail generated on Town systems, is subject to monitoring, and must not be inappropriate.

- Employees who use the Internet on personal time can enhance their knowledge of electronic information resources and sharpen information technology skills. By allowing use on personal time, the Town builds a pool of computer literate employees who can guide and encourage other employees. Personal time includes breaks, lunchtime and the time before and after scheduled work hours. Employees performing job-related use will always have priority over those desiring access to resources for personal use.

- Personal use must not interfere with the town's business needs or operation in any way and must not violate the law or any other aspect of this policy.
    - *Note: Social media sites and services such as Facebook, Twitter, and sites of a social media nature shall not be accessed from town-owned equipment unless the access is for official town business and is approved by the employee's department head or appointing authority for a public purpose. Anything posted to any social media site from town-owned equipment by a town employee must be approved by the employee's department head or appointing authority and must be for a bona-fide public purpose.*
    - Employees are cautioned that inappropriate postings to social media sites on personal time and/or using solely personal devices and accounts may subject the employee to discipline, up to and including termination, if the postings adversely effect the Town or the workplace. By way of example, and not by way of limitation, inappropriate personal postings that may subject an employee to discipline include threats of violence, comments suggesting that the employee harbors any animosity or bias towards any protected class of individuals or any individual member of a protected class, and the disclosure of personal information or other confidential information gleaned in the workplace.

- Examples of job-related use of the Internet include: accessing external databases and files to obtain reference information or conduct research; corresponding with the Town's customers and other town employees; disseminating documents to individuals or groups; and participating in discussion groups on job-related topics.

B2. Use of Technology: (Continued)

- Inappropriate use of technology includes, but is not limited to, any activity that is illegal, the creation or distribution of pornography, and activities such as political lobbying, or personal or business use to benefit those other than the Town. Examples of inappropriate use include, but are not limited to:
    - Activities that could cause congestion or disruption of the network, including downloading and installation of executable programs on the network.
    - Use of abusive or objectionable language in either public or private messages. The telecommunications systems should not be used to create any offensive or disruptive messages or images.
    - Engaging in computer gaming or gambling.
    - Accessing material or sites that contain unlawful or sexually explicit material.
    - Misrepresentation of oneself or the Town.
    - Lobbying Town Boards or elected officials to advocate for personal or extra-departmental issues.
    - Sending chain letters.
    - Using official dissemination tools to distribute personal information.

B3. Public Nature of Technology/NO EXPECTATION OF PRIVACY

- The Town reserves the right to retrieve, read, and/or analyze any electronic communication messages or any other data stored, created, received, or transmitted on Town-owned equipment.

- All data existing within the Town's Information Technology infrastructure is considered property of the Town of Hopkinton and no assumption of privacy may be made. Employees and other users of the Town of Hopkinton Information Technology infrastructure should have NO EXPECTATION OF PRIVACY with respect to their communications or other use of the technology.

- E-mail does not have the same privacy safeguards afforded regular mail or telephone communications. A good standard to apply is: Do not send an e-mail you would not want printed on the front page of the local newspaper.

B4. Operational Requirements of Technology

- Users are required to maintain the privacy of passwords and are prohibited from publishing or discussing passwords with others (except with the IT Officer or his designee).

- Should a user suspect that their password or access has been observed or compromised, the user shall immediately change their password or request assistance in doing so from the IT Officer.

- Users are forbidden from attempting to access files that are held in the realm of other users' or other departments' secure file spaces (unless they have been officially granted shared rights). Although system security should not allow this type of access to occur, if it unintentionally does occur, the user should immediately report the issue to their department head and/or the IT Officer. Any user found intentionally attempting to break into areas that they do not have rightful access to or found intentionally perusing or otherwise consuming information in such areas shall be deemed to have violated this policy.

B4. Operational Requirements of Technology (Continued)

- In order to maintain compliance to licensing and copyright law, and to increase security and reliability of systems, software installation is allowed only within the following parameters:
    - The software is licensed to the Town of Hopkinton.
    - The person installing the software is expressly authorized to do so by the IT Officer.

- In order to maintain a secure, stable and operational network, hardware and peripheral installation is allowed only within the following parameters:
    - The equipment is owned by the Town of Hopkinton and has been inventoried and accepted for use by the IT Officer.
    - The person installing the equipment is expressly authorized to do so by the IT Officer.

- Since all data within the Town of Hopkinton Information Technology infrastructure is subject to monitoring and is considered public information, attaching personal equipment (such as laptops, or flash drives) to the Town of Hopkinton IT Infrastructure is not permitted without the express authorization of the IT Officer.

- Computer users are expected to use hardware and software in a manner that enables its ongoing usage. If a piece of equipment malfunctions, the user is to notify the IT Officer in a timely manner so that the equipment may be assessed for damage and replaced or repaired. No equipment or software is to be disposed of by anyone but the IT Officer.

- All data received from sources outside the Town of Hopkinton including the Internet, floppy disk, zip disks, USB drives and tape are to be scanned for viruses. If any source is questionable, the IT Officer should be consulted prior to downloading or uploading data to Town computers.

- The IT Officer shall back up all Town data regularly and shall include off-site and disaster recovery strategies as outline in the Town's Continuity of Operations Plan.

- The IT Officer has implemented a procedure that copies ALL incoming and all Town domain (Hopkinton.org) outgoing e-mail to a central storage area. Incoming traffic includes ALL traffic generated from ANY e-mail account on ANY type of device, including handheld devices, even if such device is personally-owned – since incoming traffic to the Town is all sent to official, Hopkinton.org e-mail accounts.

- Even though a backup copy may be available, no computer user is authorized to permanently delete ANY e-mail (either incoming or outgoing) from their workstation unless the e-mail in question is clearly incoming SPAM (i.e. unsolicited bulk e-mail, usually advertising or inappropriate material, sent to large numbers of people); or the incoming e-mail in question is clearly incoming "Junk Mail" (i.e. any mail or letters that are not welcome or solicited and obviously sent in bulk; especially mail of a commercial nature such as advertising circulars, catalogues, form letters, and general marketing materials); or the incoming e-mail in question is likely or actually infected with a virus. It is not envisioned that records of outgoing e-mail would ever have a valid reason for deletion and no user shall intentionally configure the e-mail system on a Town computer or account so that copies and/or backup copies of sent messages are not generated.

B4. Operational Requirements of Technology (Continued)

- E-mails may be organized into logical folders within a user’s e-mail system and may be moved from the user’s “inbox” via the “delete” key or icon so long as the e-mail system places the message(s) in a “deleted items” or other appropriate folder (i.e. the message is just moving to another folder and not actually being deleted from the system).

- All procurement of Information Technology (as defined above) shall be made through the IT Officer, or with his permission.

- Employees must have written permission from the IT Officer to remove from Town offices Town-owned technological devices of any kind and must sign a statement identifying all of the equipment in question and indicating that they are responsible for the well-being of the equipment and the safeguarding of any data stored thereupon.

- All computer repairs will be made on Town property, with limited exceptions, to ensure that confidential data has adequate controls.

- Employees are permitted to monitor Town e-mail using personal devices. However, for those employees who have a Town-issued, Town-owned computer in the work environment, all such activity must ensure that copies of incoming e-mail are kept on the Town’s hosted e-mail server until it can be downloaded using the employee’s Town-issued equipment that exists in the work environment the next time they access their e-mail at work. Employees shall also ensure that personal information is safeguarded on their personal devices if the source of that information is the Town’s e-mail system or IT infrastructure. Further, all provisions of the Public Records Law and this policy apply as well to personal devices used to transmit, receive, create, or store information for public purposes.