



TOWN OF HILLSBOROUGH

PERSONNEL POLICY

POLICY 222

CREATED 9/12/2022

SUBJECT: ELECTRONIC COMMUNICATION, INTERNET, AND EMAIL USAGE

PURPOSE: To establish an Electronic Communication, Internet, and Email Usage policy to ensure the Town meets its legal obligations and to protect computer and information technology system security and Town property rights.

STATEMENT OF POLICY:

Electronic mail, internet usage, and other electronic communications are considered an integral part of the working environment, whether the work is being performed on-site or remotely pursuant to an approved telework arrangement. The following types of electronic communications and equipment are the property and/or records of the Town:

- Telephones, Town-owned cellular phones & voicemail facilities
- Town e-mail accounts and all e-mails sent and received by them.
- Fax machines, modems, and servers
- Town-supplied computers
- Network tools such as Internet access while using Town equipment or systems

The Town reserves the right to access and disclose all messages sent over its e-mail system(s) for any purpose.

USAGE OF TOWN EQUIPMENT OR SYSTEMS; PRIVACY AND CONFIDENTIALITY

All messages composed, sent, or received through electronic communications systems, and all Internet connections to web sites using Town equipment or systems, are and remain the property of the Town. They are NOT the private property of any employee and should not be considered private. The Town reserves and intends to exercise the right to review, audit, intercept, access, print, read, and disclose all messages created, received, or sent through its electronic communication systems, including the e-mail network, for any purpose. Internet access and use of e-mail systems is not confidential, and employees shall therefore have no expectation of privacy in anything that is reviewed, viewed, or downloaded from the Town's network

or using Town equipment/systems. Please note that even when a message is deleted, it is still possible to recreate the message, and the ultimate privacy of messages cannot be guaranteed to anyone. Employees are not to access a file or retrieve any stored communication without authorization.

Except as otherwise noted, all messages transmitted over the Town's e-mail system will be considered Town business activities and should only contain information essential for the accomplishment of Town business, administration, or practices. Town business should be conducted using exclusively Town email and messaging systems, and not through personal email accounts, apps, or other electronic systems. It is a violation of this policy for any employee, including system administrators, supervisors, or programmers to use Town e-mail and computer systems for purposes of satisfying idle curiosity about the affairs of others, with no substantial business purpose for obtaining access to the files or communications of others.

In certain approved situations, employees may receive confidential work-related emails from outside parties, i.e. Police Officers receiving confidential information from the federal government. In such situations, employees must continue to maintain the confidentiality of that information and should not disclose it to or make it available to anyone who is not authorized to review or receive such information. If you have a question about this, please contact Human Resources or your supervisor.

PASSWORDS:

All users must utilize a password-protected connection for Town business, provide the appropriate designated supervisor with any such password(s) in the event the employee is absent for any reason, and notify the Administrator of any password changes when made. The reliability of passwords for maintaining confidentiality cannot be guaranteed. You must assume that any and all messages may be read by someone other than the intended or designated recipient. All connections made through the Town's Internet connection are considered Town business activities, and the viewing, reviewing, printing, or saving of information received from the Internet should follow all Town business administration rules or practices.

Employees are prohibited from disclosing their voice or e-mail access password(s), or those of any other employee, to anyone who is not an employee of the Town. Disclosure of passwords to other employees only should occur when required by an urgent business matter as directed by management. In such cases, passwords should be changed as soon as possible after the urgent business matter has been resolved. Passwords never should be given out over the phone, included in voice or e-mail messages posted or kept within public view.

ACCEPTABLE INTERNET AND COMMUNICATIONS SYSTEM USAGE:

Except as otherwise specifically discussed in other Town policies, the use of the electronic communications system is reserved solely for the conduct of business at

the Town. It is NOT intended to be used for personal business, and employees have no expectation of privacy when using the Town's electronic equipment or communications systems. Employees accessing the Internet, the Town's Intranet, or World Wide Web represent the Town when doing so. Accordingly, all such communications should be for professional reasons related to Town business. Each employee is responsible for ensuring that he or she uses his or her Internet access privilege in an effective, responsible, ethical and lawful manner.

Examples of typical and appropriate uses of Internet service while at work include day-to-day work activities, such as researching information for a specific department or division or using an authorized website to purchase goods and services from Town vendors. Incidental and occasional personal use of the Town's e-mail system for essential brief personal matters that cannot be handled during non-working hours is permitted. However, employees should be aware that these messages are subject to the access and disclosure rights of the Town. Employees are therefore expected to keep such personal use to a minimum.

Employees are also permitted to use the Internet during their rest breaks and meal periods, consistent with the provisions below. Non-business uses should not involve significant use of the Town's electronic resources, such as others' work time, computer time, or bandwidth.

Non-business use is subject to the following:

- a. All non-business communications are subject to this policy in its entirety and to all other Town policies. All non-business communications may be monitored at any time in accordance with this policy.
- b. You should not use the Town's Internet for communications that you wish to keep private, such as communications with a physician or your personal attorney; keep in mind that employees have no expectation of privacy in the Town's e-mail system, whether used at the worksite or during an approved telework arrangement. If you nevertheless use the Town e-mail system to communicate with a personal attorney, or for any other communication to which an evidentiary privilege might attach, you understand that you are waiving any such privilege or confidentiality in that communication.
- c. Non-business uses should only occur during rest breaks or lunch periods. Consistent with the Town's policies regarding rest breaks and meal periods, employees should not be interrupted during such unpaid breaks. If an employee decides to use the Internet during his/her rest break and/or meal period, the employee is not to perform any work during this period, including responding to work related e-mails, telephone calls, etc.
- d. Non-business uses do not preempt any business activity and must not interfere with the user's or others' productivity.

- e. Employees' access to personal e-mail accounts is subject to all of the requirements contained in this policy.

Non-exempt employees must not review or send e-mails, voicemails, or text messages, make phone calls, or engage in any other work or work-related activities outside their scheduled work time without prior authorization.

The Town reserves the right to periodically review all Internet connections made by its personnel, and inspect and search its computers, networks, and systems, to ensure compliance with this policy and all other Town policies. Such review can be conducted during or after business hours and in the presence or absence of the employee. For purposes of inspecting, investigating, or searching employees' files or documents, the Town may override any applicable passwords, codes, or locks in accordance with the best interests of the Town, its employees, and its clients or visitors. The Town hereby notifies all employees that it has access to internet connection database systems and may exercise that access at any time, for any reason, and without employee permission or knowledge, including for the following purposes:

- a. Investigation of actual or suspected impropriety or violation of Town policy.
- b. Compliance with legal requirements.
- c. Investigation of actual or suspected criminal activities.
- d. Breach of security.
- e. To review any individual's overall use of the Internet.
- f. Performance of routine maintenance.
- g. Protection of system security or Town property rights.

PROHIBITED INTERNET AND COMMUNICATION SYSTEM USAGE:

The Internet and Town electronic communication systems shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or other confidential materials without prior authorization. The Town purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the Town does not have the right to reproduce such software for use on more than one computer. Employees may only use software on local area networks or on multiple machines according to the software license agreement. The Town prohibits the illegal duplication of software and its related documentation.

Employees may access only messages, files or programs, whether computerized or not, that they have permission to enter. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems or programs, voicemail messages or other property of the Town, or improper use of information obtained by authorized means, will be grounds for disciplinary action, up to and including termination.

Employees should use common sense and manners when using the Internet and composing e-mail messages. Periodically, due to the nature of the web and its interconnection (links) to other sites, employees may inadvertently be placed in a position of violating this policy. It is your responsibility to not linger and move on to an appropriate site, as well as to promptly report unexpected “pop up” sites or other non-compliant material to your supervisor or IT.

Employees may not access websites that are offensive, subversive, immoral, and pornographic, or that are in conflict with Town policies or generally accepted standards of business decorum. A general guideline for use would be to consider whether a supervisor or department manager would approve of accessing a specific website or Internet resource. Use of insulting, offensive, disrespectful, demeaning, or sexually suggestive language will not be tolerated. Harassment in any form, obscenities, any representation of obscenities, or sexual, religious, or ethnic slurs will not be tolerated. Sending a copy of these types of offensive emails to a separate party will not be tolerated, except in the performance of official law enforcement duties. Employees may be subject to disciplinary action for violations of this policy.

The Town is prohibited from assisting employees with any private profit-making activity utilizing a website, and accordingly, no employee may post or access any non-business private, for-sale, or want ads using Town Internet or communication services.

Correspondence with, or access to, any website of a political nature is prohibited. (See the Town’s political activity policy for additional information).

Correspondence with, or access to, any website of a religious nature or that promotes or opposes any religious belief is prohibited.

USAGE GUIDELINES FOR TOWN E-MAIL SERVICE:

All employees with Town e-mail accounts are responsible for the management of their own inbox and associated folders. All e-mail users must utilize a password, in accordance with the rules for passwords set forth above.

The Town’s e-mail system uses two-factor authentication, which requires a second code to be entered upon login for security purposes. For those employees who receive a cell phone allowance, this second code will be sent to the employee’s cell phone. For those employees who do not receive a cell phone allowance, a device

(key) will be issued to each person which can be used to access the second code. This “key” device will be provided by the Town—however, if an employee loses or damages a “key,” the employee will be charged \$20 to replace it.

E-mail should not be used for network-wide or broadcast purposes, unless the user genuinely believes the message is of interest to all intended recipients.

Training on e-mail usage will be provided as an employee’s access to the Town’s network becomes available. Employees will be provided an opportunity to attend a workshop or other arrangement for training may be provided. It is the responsibility of the employee to be properly trained on the use of e-mail and Town communication systems.

The Town has access to any and all electronic mail stored on its information systems, except where law enforcement exceptions apply such as the CLETS system, NCRIC, and other protected information, and may exercise that access at any time, for any reason, including:

- a. Investigation of actual or suspected impropriety or violation of Town policy.
- b. Legal requirements.
- c. Investigation of actual or suspected criminal activities.
- d. Breach of electronic mail security.
- e. To locate substantive information that is not more readily available by some other means.
- f. For the performance of routine maintenance.

The Town reserves the right to disclose the contents of such electronic communications within or outside the Town without employee permission or knowledge. The Town has unlimited access to such electronic communications to protect information system security and the Town’s property rights.

The fact that e-mail is available as a tool to employees does not mean it is the *right* tool for various forms of sensitive communications. Some information should be discussed in person or by phone/virtual meeting; some information should be transmitted through formal business correspondence. The Town expects employees to be mindful of the type of communication being sent and whether email is the best method.

E-mail and related communication records are public records under California law and may need to be disclosed in accordance with the California Public Records Act and other applicable statutes.

COMPLIANCE WITH OTHER TOWN POLICIES AND RULES:

All electronic communications shall comply with all Town policies and rules, including but not limited to the Unlawful Discrimination / Harassment / Retaliation Policy, and the Town's Solicitation / Distribution regulations. In no circumstances are the electronic communication systems to be used to create any offensive or disruptive messages, or any message that might constitute (or indicate the condoning or encouragement of) harassment, lewd, illicit or illegal activities. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability. The electronic communication systems may not be used to solicit for commercial ventures, religious or political causes, outside organizations or other non job related solicitations. Employees learning of any misuse of the voicemail / e-mail system or violations of this policy shall notify Human Resources.

ELECTRONIC COMMUNICATIONS THROUGH THIRD PARTY SERVICE PROVIDERS:

Town business generally should be conducted using the Town's electronic resources. Unless pre-approved in writing by the City Manager, employees should not use personal e-mail accounts, cell phones, or personal digital assistants to conduct any Town business. The Town may need access to information stored on those devices or with the third-party service provider for the Town's legitimate business purposes. These employees, therefore, should understand that the Town may request that the employee search their personal communication device for any such communications, or request that the employee work with the third-party service provider to disclose to the Town the content of stored communications concerning the Town's business. An employee's refusal to comply with the Town's request to search for such communications may result in discipline up through and including termination. Employees are required to cooperate with the Town in obtaining such consent as well as in the Town's obtaining access to the stored communications.

Communications by employees through any third-party electronic communications service for which the Town is the subscriber or for which it pays the subscription directly or through reimbursement to the employee are subject to all Town policies, including this policy.