Technology Use Policy

Objective:

The City is a strong proponent of the use of technology to optimize efforts in conducting City business. The City's ability to use these tools will greatly enhance its mission and should make staff more efficient when dealing with information gathering and exchange. The City encourages all employees to use technology to increase productivity and efficiency. This policy is to ensure that the use of such technologies among City employees is consistent with other City policies, all applicable laws, and the individual user's job responsibilities.

This policy applies to all City employees, vendors, contractors, interns, volunteers, and otherwise defined entities that use City technology assets and equipment. This policy applies to remote use such as virtual private networking (VPN), wireless, and other remote access technologies. In general, City employees have an obligation to use City technology in a responsible and informed manner just as any other business asset of the City is used. The following policies have been developed to provide a framework for appropriate use by all City employees.

- By using City-provided technology assets and equipment, employees acknowledge and agree that they have no expectation of privacy or confidentiality in the use of these tools, or in any data that they create, store, or transmit on or over these tools, including any data created, stored or transmitted during an employee's incidental personal use of these tools as permitted under this policy. They are provided solely for the purpose of conducting City business and should be used as such. Access to any information stored on the city network, data store or device can be obtained by the request of a supervisor in doing authorized business to the Information and Technologies Supervisor or the Human Resource division. Employees should understand that certain email messages, other electronic communications, and documents created on City computer systems may be considered a public record subject to disclosure and/or subject to discovery in the event of litigation.

- Departments are permitted to issue their own policies that augment this policy. In some cases it may be necessary to be more restrictive than this policy, however in no case may other adopted policies be less restrictive.
- Downloading software programs of any kind may subject the computer and the network to viruses or other malicious software, which can destroy or compromise data on the computer and the network. Thus, software shall not be downloaded (nor installed) without the prior approval of the I.T. Manager or his delegate. Connecting non-City provided equipment to the City's network can introduce significant hazards to City technology assets. No City employee, intern, volunteer, vendor, contractor, or otherwise defined entity shall connect a non-City owned device of any kind to the City network or technology assets in any fashion without prior consent of the I.T. Manager.
- Not all employees have access to City technology assets such as e-mail or Internet access and this policy does not create a right to have such access. City staff shall not provide access to those who have not been given explicit authorization to access City technology such as friends or family members.
- The City implements security measures around its technology to mitigate the risk of utilizing network technologies such as the Internet. Examples of security measures include usernames and passwords. City staff shall not share this information or store this information in an unsecure fashion. Should City staff have any knowledge of a security risk such as the loss of a City technology asset or compromised usernames and passwords, the IT Division must be notified immediately.
- Violations of this policy may subject an employee to the City's disciplinary policy.

Employee Responsibilities:

Monitor personal use of the internet, messaging, and other applications, to ensure that the City is being appropriately served. Adhere to City standards as discussed in this policy. Read and adhere to relevant policies. Obtain authorization from their supervisor before incurring charges; for example, downloading data or accessing a paid service.

Request Information and Technology staff to download and install software unless express consent has been granted for employees to download and install software.

Management Responsibilities:

Ensure that the primary purpose of technology use is to meet City business needs, and that relevant City standards are met. Review and make decisions regarding the approval of all non-work related broadcast announcements. Acceptable uses for non-work related broadcast announcements would include arrival or departure of a department employee or a departmental charitable campaign event. Promptly notify I.T. of any addition or termination from the work force.

Internet Use and Issues:

The Internet is a publicly accessible highly unregulated network that spans international lines and laws and has billions of connected people and resources. This provides an enormously rich and productive tool for City staff to utilize in many different ways. It also has many hazards that must be taken into consideration to protect the City and staff from liability.

Guidelines on Official Use of the Internet:

- The Internet is not a secure means of transmission. Thus, sensitive or confidential files or e-mail should not be sent over the Internet.
- Unless you are specifically authorized to do so, do not claim to represent the views or positions of the City.

Unacceptable sites or Internet uses include, but are not limited to, the following:

- Pornographic sites and access to pornographic materials.
- Sites which promote exclusivity, hatred, or positions which are contrary to the City’s policy of embracing cultural diversity.
- Internet use to harass anyone - employees, vendors, customers, and others.
- Online interactive sports or games sites.

- Sites that promote illegal activity.
- Social Networking or Dating sites not specifically related to your job function
- Internet use for political purposes.
- Unauthorized transfer of copyrighted materials.
- Any site that charges a fee (unless there has been prior written approval to justify the City expense for the item by the supervisor or the department Director).
- Marketing of personal or private business.
- Participation in non-business Internet discussion groups or chat rooms.
- Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace.
- Sharing or storing unlicensed software or audio/video files.
- Using a City e-mail address when posting to public forums e.g. blogs, social media sites, wikis and discussion lists for personal use.
- Accessing sites that distribute computer security exploits ("hacking" sites).

Guidelines on Personal Use of the Internet:

The use of electronic equipment provided by the City is for the purposes of conducting City business. However, de minimus personal use of e-mail and the Internet is permissible if it is utilized on a limited basis and in such a way that it does not interfere with the employee's responsibilities or official City business nor pose any risk or inflict damage on City technology assets. Generally speaking, de minimus personal use means: (1) it is occasional and of short duration; (2) it is done on an employee's personal time, such as on a lunch break; (3) it does not interfere with job responsibilities; (4) it does not result in any expense to the City; (5) it does not solicit for or promote commercial ventures; (6) it does not utilize excessive network resources; and (7) it does not constitute any prohibited use, as discussed in this policy. Such use must not interfere with official business and if there is any doubt about whether the use is de minimus or if there is an expense, employees should consult their supervisor or the I.T. Manager. Authorized de minimus personal use of the Internet is a concept that recognizes the reality of the workplace. Employees have a legitimate need at times to contact family, friends, and take care of a certain amount of personal business during the workday. City employees are expected to observe the following guidelines on personal Internet use:

- Employees must limit the personal use of the Internet to occasional and short duration and during personal time (during breaks or before/after work hours).
- Personal use of the Internet must not adversely reflect on the City (e.g., furthering of extremist organizations; dirty jokes; chain letters; racial ethnic or gender slurs).
- Unlawful or inappropriate use of the Internet is not permitted (e.g., no access to pornographic sites, no privacy violations, no release of confidential, sensitive, classified, or public disclosure exempt information, no copyright or licensing law violations).
- Employees may transact a limited amount of commercial activities on the Internet at work, but may not conduct a business through the Internet (e.g., purchase of a book through the Internet is acceptable, but conducting a consultant business while at work is not).
- Personal use of the Internet must not interfere with the City's mission.
- Employees must not use the Internet for political activities (e.g., using Internet to further one's own or someone else's political campaign).
- Employees may not claim to represent the views or positions of the City, and may not make any unauthorized commitments or promises of any kind purporting to bind the City.
- If employees accidentally access a website that contains pornographic, sexually explicit, inappropriate or illegal materials, they must leave the site immediately.
- Supervisors are responsible for determining reasonableness of use and may restrict an employee's access to the Internet, e-mail, or other computer programs.

Electronic Mail (e-mail):

- The e-mail system may not be used to solicit or generate interest in commercial ventures, chain letters, religious or political causes, outside organizations, or other non-job-related solicitations.

- The e-mail system may not be used to access, create, or forward offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual content, racial slurs, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
- The e-mail system and the Internet may not be used to send (upload) or receive (download) copyrighted materials. All licensing conditions, downloading and usage conditions should be understood before using or distributing any copyrighted information.
- All email generated or received on the City's email system is archived. This includes emails that have been deleted, forwarded, created, sent, and any other potential state of an email. This means that all email can be potentially requested in a records request. Employees email messages may be reviewed or audited at any time by any supervisor upon order of management staff. City staff should be aware of this and conduct email activities accordingly.
- All email used to broadcast mail to large numbers of constituents must use the BCC field to hide all email addresses.
- It is expected that all e-mail messages, regardless of the recipient will be professional in content.

Authorized Users:

No City employee shall be authorized to use City technology assets until he or she has signed a document indicating that the employee has read and agrees to be bound by the terms of this policy.

Directories and File Structure:

For security reasons and to provide consistent backups, files are to be saved on the network not on the employee's computer. Directories and files on the network are backed up on a nightly basis. All data not saved to the network will not be backed up and the employee will be responsible for loss of data in the event of a hardware failure. To have a file restored from a backup, contact the I.T. Division.

Each department has access to a shared network drive which all other departments have access to. At this level the shares are considered “public” in that everyone with access to the network can view files located here. There are also many shares which are specific to a team or group which are restricted but provide an efficient way of sharing files between staff. The City also provides each user with a “private or H” drive in which they can store their files on the network. This H drive is only accessible to the user and is also backed up every night.

Employees are expected to periodically review the files they have saved on the network to determine if they are still useful and delete files that are no longer needed.

Backup and Recovery:

A full backup of the entire network is done on a nightly basis. All critical files should be saved to the network so they are backed up. This ensures that inadvertently deleted or corrupted files can be restored from back-up and will not need to be re-created. It is the responsibility of the employee to save critical files on the network.

Software:

All software will be legally licensed to the City of Fife and not in the individual employee’s name.

The City will purchase the required number of licenses required to meet the software vendor’s requirements.

Employees are not authorized to install personal software (software not purchased by the City) on their computers without the express consent of the I.T. Manager.

Enforcement of Policy:

Violation of any part of this policy shall be subject to disciplinary action up to and including termination. It is the Department Director’s responsibility to enforce these policies. Employees who are found in violation of this policy may be subject to the following:

- Internet and E-Mail access may be revoked

- Access times may be restricted
- Disciplinary action

Password Policy:

Objective: Usernames, passwords and PIN's are one of the most basic and critical lines of defense against unauthorized activity on the City's network and computer equipment. A strong password helps mitigate risk against unauthorized activity and attacks such as dictionary password and brute force password hacks. As a government agency the City is also required to abide by policies related to regional, state, and federal networks. This policy's intent is to establish parameters that are required in each authorized user's password.

Users must choose their own passwords and it must conform to the following criteria:

- Must be a minimum length of seven (7) characters on all systems.
- Must not be the same as the User id.
- Must contain at least one special character.
- Expires with a maximum of 90 calendar days.
- Not be transmitted in the clear outside the network.
- Not be displayed when entered.
- If a user believes their password has been compromised, the user must contact the Fife IT division immediately for assistance.
- All accounts will be automatically disabled for 30 minutes after 3 unsuccessful logon attempts.

PIN'S

PIN's are Personal Identification Numbers used to lock smartphones, voice mail, and other devices that contain secure data. Like passwords users should be using hard-to-guess combinations.

Users must choose their own PIN's and it must conform to the following criteria:

- Must not be the same as the User id. Example: If you extension is 8674 then your password should not also be 8674.
- Must contain at least three different numbers. Example: Your password can not be 0000, 1111, 5555............
- Should not make a line across the keypad. Example: 2580 goes down the center row of a telephone and shouldn't be used.
- Should not be a simple pattern of acceding or descending numbers. Example: 1234 or 9876.

If a user forgets their PIN simply contact the Fife IT division for assistance.

Terminated Employees:

The City periodically terminates employment relationships for a variety of reasons with staff as part of normal business operations. As such the following steps will be taken to prevent un-authorized access to the City's network and computer resources from terminated employees.

- Once a termination of employment effective date has been set the supervisor, manager, HR, or Director of the employee will contact the I.T. Team to inform them of termination date, with whom access to the terminated employee's digital content should be transferred to, and whether the position is going to be re-filled.
- The I.T. Team will ensure that all access to network and computer resources is removed on the effective date of employment termination with the exception of the designated staff person who is to receive access to the terminated employee's digital content.

The I.T. Team will also conduct an informal audit during quarterly maintenance cycles to ensure that un-authorized user accounts have been properly removed.