Use of Technology Administrative Procedure

Procedure Name: Use of Technology Administrative Procedure
Last Updated: July 7, 2023
Service Area Lead: Director, Information Technology Services

1. Procedure Statement

To identify acceptable use, restrictions on use, and usage procedures for all those using Corporate Technology.

This Policy also applies to the components, systems, software, and hardware related to Corporate Technology including, but not limited to, the internet, electronic messaging such as email, and other media and social networking sites.

2. Definitions

2.1. Corporate Technology: includes, but is not limited to: software, desktop computers, laptops, tablet or pad style computers, telephones, wireless handheld devices, mobile media such as USB keys, cellular phones, smartphones, printers, scanners, photocopiers, building automation systems and components, Internet based “Software as a Service” (SaaS) applications, fax machines, as well as messaging systems such as email, instant messaging, social media, SMS and MMS text, PIN to PIN, voice and voicemail, and any other technology provided by or accessed through the Corporation (including internet-based systems and services).

Corporate Technology includes Internet and intranet web sites published and branded to be identified with the City of London.

Corporate Technology includes Operational Technology building automation components such as HVAC systems which may incorporate network connected components.

3. Applicability

This Procedure applies to all Corporation employees and other users (non-Corporation employees, volunteers and/or contractors, as well as clients who are authorized to use or have access to Corporate Technology). This Policy applies to usage during and outside work hours.

4. The Procedure

4.1. Overall Principles:

1. Corporate Technology is provided to improve productivity and facilitate the business activities of the Corporation. Every employee and user of Corporate Technology is responsible for ensuring such technology is used in an appropriate manner in accordance with this Policy and all other applicable Corporation policies.

2. Corporate Technology is provided for Corporation business purposes and is not intended for personal use. Incidental and occasional personal use of Corporate Technology is permitted, provided such limited use:

- Does not result in any unauthorized expense to the Corporation including time or materials;
- Does not interfere with and/or negatively impact productivity;
- Does not interfere and/or conflict with the intended business uses of Corporate Technology;
- Is not for illegal purposes, or to gather or transmit information to support illegal activities;
- Is in accordance with all applicable laws, regulations, and/or by-laws;

- Complies with this and all other applicable Corporation policies including but not limited to: corporate Information Security policies; the Respectful Workplace Policy; the Workplace Violence Prevention Policy; and the corporate Procurement of Goods and Services Policy.

Under no circumstances is Corporate Technology to be used for accessing sites for viewing, accessing, downloading, storing, and/or distribution (via email, hardcopy, images, texts, video clips or otherwise) of inappropriate material, as determined by the Corporation. Inappropriate material includes, but is not limited to, sites containing material which is obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material), racially offensive/degrading, defamatory, discriminatory, hate propaganda or otherwise inappropriate as determined by the Corporation.

3. Monitoring (including random spot checks) and reporting of abuses of this Procedure is a function of Information Technology Services.

   All computer network traffic (including email and internet activity) and data stored on all storage mediums is subject to random inspection. Information Technology Services will monitor computer related activities on a random basis, or upon management's request for various purposes, including but not limited to, technical maintenance and repair, production of Corporate records, to improve business processes and manage productivity, to prevent employee misconduct and ensure compliance with the law and Corporate policies. All communications, including those marked confidential and/or personal may be monitored by the Corporation.

   Employees and other users shall not have any expectation of privacy when using Corporate Technology whether for business or personal use. With the authorization of the Director, People Services or the Director, Information Technology Services or their designates, the Corporation may access or monitor individual user activities, internet usage, files, including archived and "deleted" material of present and former employees, without the user's consent or knowledge.

   The use of Corporate Technology for personal use in accordance with this Procedure is the choice of employees and other users. If a private means of accessing, creating and/or communicating information for personal use is required or desired, a personal technological device unconnected to Corporate Technology or the Corporation's network should be used.

4. All documents created through the use of and/or retained on Corporate Technology, whether for business or personal use, including, but not limited to, emails and other communications may be subject to the access and privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA"). All such documents and communications shall therefore be managed by employees in accordance with MFIPPA and in accordance with any restrictions placed upon their use by the Corporation, by the sender of the communication or by the creator/supplier of the document.

5. Information or data cannot be copied to mobile media (e.g., USB key, CD/DVD and personal devices such as MP3 recorders) or communicated electronically

to another individual, agency, public or private corporation, for any purpose other than approved Corporate business. Should an employee have any doubt about the appropriateness of a request for information, the advice of their manager and/or the Corporation's Municipal Freedom of Information and Protection of Privacy Act Head shall be obtained.

6. Corporate Technology cannot be used for any activity for which an employee receives remuneration or "in-kind" service or other personal benefit other than that received directly from the Corporation, whether during or outside work hours.

7. No computer software, hardware and/or telecommunications equipment (including internet or intranet web sites, or internet-based "cloud" Software as a Service SaaS applications and systems) will be purchased, installed, or deployed without the completion of appropriate Information Security and technology reviews as determined by Information Technology Services and the expressed authorization, in writing, of the Director, Information Technology Services or designate.

8. New Corporate Technology proposed for use in the corporation must be submitted in accordance with the procedures and processes of the Technology Investment Strategy committee.

9. Employees and other users of Corporate Technology are prohibited from uninstalling, modifying, or otherwise disabling any technology installed on computers or other devices that have been installed by the Corporation unless expressly authorized in writing by the Director, Information Technology Services or designate to do so.

10. Employees and other users bringing personal computers or other technology into the workplace shall ensure their use of such devices is in compliance with this and all other applicable Corporate policies.

    Employees shall not connect personal computers or other personal technology to Corporate Technology unless expressly authorized in writing by the Director, Information Technology Services or designate.

11. Employees and other users accessing Corporate Technology remotely, whether during or outside work hours, are required to comply with this Procedure and all other applicable Corporate policies with respect to the use of Corporate Technology.

12. All employees have a responsibility to report policy and procedure violations to their manager. Managers then have a responsibility to report such matters to both People Services and Information Technology Services. Inappropriate, irregular, and/or suspicious activities must be reported by managers to the Director, People Services or designate, and the Director, Information Technology Services or designate. Monitoring and reporting of abuses of this Policy will not distinguish between business and personal use.

13. All Corporate Technology must be returned to Information Technology Services when an employee departs the Corporation. If an employee is on an extended leave of absence, access to Corporate Systems will be removed and Corporate Technology must be returned to Information Technology Services.

14. The Corporation, in its sole discretion, reserves the right to:
    - Remove or limit any user's use of and/or access to Corporate Technology;
    - Block internet access, entirely or in part, for all users, specific users, and/or locations;
    - Restrict access to some or all social networking sites through Corporate Technology; and

- Take any other measures it deems necessary to protect the confidentiality, integrity, and availability of Corporate Technology, including but not limited to mandating the completion of training on safe use of such systems.

15. All Corporate Technology must undergo an initial information security assessment prior to production usage, and periodic re-assessments after major updates to the technology. Technology providers will be required to remediate vulnerabilities identified in the technology prior to production usage, with acceptance of outstanding risks at the discretion of the Director, Information Technology Services. This assessment may be waived by the Director, Information Technology Services upon presentation of attestation that the vendor is certified to internationally recognized security certification standards and has periodic re-assessments of the technology performed by an accredited independent assessor.

    This security assessment requirement also applies to Internet or intranet web sites and "cloud" based Software as a Service (SaaS) applications which are not installed on City computers but are accessed on the Internet from Corporate Technology devices. Such applications must be approved for use, assessed before production usage, and re-assessed on an annual basis in accordance with the SaaS Application Lifecycle Management administrative procedure.

4.2. Mobile Equipment:

Employees who are assigned portable Corporate Technology must use Multi-factor Authentication (MFA) to securely authenticate to Corporate Services.

Employees in possession of portable Corporate Technology equipment must not leave it unattended at any time when outside Corporate facilities unless it has been secured.

All cases of loss or theft of portable Corporate Technology must be reported to Information Technology Services immediately.

4.3. Software Licenses and Copyrights:

All software installed or used on any Corporate Technology equipment must have a valid license. This includes freeware and shareware programs obtained from the internet and/or other sources. All non-standard software must also be approved in writing for use in the Corporation environment by the Director, Information Technology Services or designate.

Licensed software shall be used in compliance with the manufacturer's intended usage and according to the legally licensed copyright and must not be copied or duplicated, except as explicitly allowed in the license terms and conditions. No programs or files from an external source (including the internet), licensed or unlicensed, are to be personally obtained and installed unless it has been investigated and approved in writing by the Director, Information Technology Services or designate. This Procedure likewise applies to text, images, audio, and all other manner of copyrighted materials.

4.4. Social Media:

Employees are reminded that even though they are using social media for personal purposes, some Corporation policies, including, but not limited to, the Respectful Workplace Policy, Code of Conduct for Employees, and the Workplace Violence Prevention Policy may be applicable to off duty conduct.

Employees using social media for personal purposes, whether using Corporate Technology or personal devices, should consider the following:

- An individual using social media may be identified as a Corporation employee by the posting of their name, their place of work, their photograph, or by content they post;
- Employees must avoid placing themselves in a conflict of interest including revealing confidential or privileged Corporate information, or personal information gained through work such as client or employee information.
- Employees must abide by the Respectful Workplace Policy, Code of Conduct for Employees, and the Workplace Violence Prevention Policy;
- Employees should not identify and comment about other Corporation employees without their consent.
- Employees should avoid the appearance of officially representing the Corporation on their personal sites or account. They must avoid posting Corporate owned identities including logos, photographs, graphics, or other media without Corporate Communications' written authorization.
- Only employees authorized in writing as Social Media Moderators by Corporate Communications can participate in social media communications on behalf of the Corporation in accordance with the Social Media Procedure.

4.5. Passwords and Other Login Security:

Every user of Corporate Technology is provided with a user ID. Associated with each user-ID is a password, which must be used to authenticate the person accessing the application, system, network, and remote connections. Passwords must be treated as confidential information and must not be disclosed or stored in places where they can be easily accessible by unauthorized people. Passwords must not be shared, unless there are exceptional and legitimate business reasons, in which case the approval of the Director, People Services, and Director, Information Technology Services, or their designates, must be received. In such cases, the employee should thereafter change their password as soon as reasonable. All individuals are responsible for all activity performed under their user-ID. Generic Accounts will not be issued unless a full ITS review has been completed and written sign-off from the Director, Information Technology Services is received.

Passwords will conform to Corporate standards as defined by Information Technology Services, which may change from time to time.

Passwords are primarily intended for purposes of securing Corporation records and information and to identify users of Corporate Technology. Passwords are not intended to preclude the Corporation's access to Corporate Technology.

Beyond passwords, the Corporation may require the use of additional or alternate login security measures to further secure access to Corporate Technology. Any such additional login security measures used for alternate and/or multi-factor authentication are subject to the same requirements as passwords.

4.6 Screensavers:

Each user-ID and/or computer will utilize a screensaver which will lock the computer in use after a specified period of inactivity. Exceptions to this Procedure will only be considered by providing a written business case to the Director, Information Technology Services explaining the need. Written approval from the Director, Information Technology Services or delegate is required for such an exception.

4.7. Storage of Files on Local Drives:

All Corporate files must be stored in accordance with the Records Retention Policy and in CityHub, OneDrive or a Corporately provided network drive to ensure they are backed up. The storage of Corporate files on local drives is not

permitted unless CityHub, OneDrive and\or Corporate network drive(s) are unavailable. Local drives are not backed up and the Corporation accepts no responsibility for their protection.

4.8. Storage of Personal Files:

The storage of personal files on network drives is not permitted. This includes MP3 and other audio files, MPEG and other video files, and JPEGs and other photography file formats.

Local drives are not backed up and the Corporation accepts no responsibility for their protection. Additionally, when a computer is replaced due to the end of its lease or for other reasons, it will be the responsibility of the employee to transfer any personal files. Information Technology Services will not be responsible for transferring personal files to a new computer.

4.9. Internet:

Internet access is a Corporate resource provided to employees and other users for research or system support purposes relevant to the Corporation's business and to provide such information to residents, potential residents, businesses, business prospects, etc.

Employees **shall not**:

- Access internet sites that contain material which is: obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material); racially offensive/degrading; defamatory; discriminatory; hate propaganda or which is otherwise inappropriate as determined by the Corporation, without the express written authorization of the Director, People Services or designate. Where an objectionable or inappropriate site is accessed accidentally, the employee shall report, in writing, such access to his or her manager and/or Information Technology Services as soon as possible;

- Send or receive any material which is: obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material); racially offensive/degrading; defamatory; discriminatory; hate propaganda; annoying; harassing, intimidating, or threatens another person or group of persons, or which is otherwise inappropriate as determined by the Corporation without the express written authorization of the Director, People Services or designate. Where an employee unwillingly receives material of this nature, he or she shall report it, in writing, to his or her manager and/or Information Technology Services as soon as possible;

- Access, download, view, store, or distribute (via email, hardcopy, images, text, video clips, or otherwise), any material which is: obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material); racially offensive/degrading; defamatory; discriminatory; hate propaganda; harassing; threatening, or which is otherwise inappropriate (including jokes, images or video clips) as determined by the Corporation, without the express written authorization of the Director, People Services or designate.

Executable software may not be downloaded without written authorization from the employee's manager and the Director, Information Technology Services or designate. Downloading of non-executable files for business use is permitted where appropriate and meets the criteria outlined in this Procedure. These

include, but are not limited to, reports, Adobe “PDF” files, spreadsheets, information flyers, etc.

Each manager is responsible for their respective employees’ use of the internet. The Director, People Services and/or the Director, Information Technology Services or their designates, subject to any other applicable Corporate policies, will co-ordinate any action as a result of abuse of internet privileges.

4.10. Email and Other Messaging Systems:

Email and other messaging system records are like any other records that are created to correspond with customers and co-workers. Professional business practices and applicable Corporate policies shall be adhered to in the creation and content of email and other messaging system records.

The following guidelines shall be adhered to:

- Use only business-like language;
- Do not express personal opinions about individuals or situations, unless it is a specific task or requirement as part of your position or job function;
- In general, do not include any text or information that would not be suitable under this and other Corporate policies. Confidential information should not be included unless it is necessary for Corporate business purposes. If there is a need to include confidential information, clearly mark your text as “confidential”. For example, in a property file, if a price is suggested in an Offer of Purchase that the City might be making to an owner, the text shall be marked as “confidential”; text containing or commenting upon legal opinion or strategy shall be marked “privileged and confidential” and should not be forwarded to co-workers or others within the Corporation unless express authorization to do so is first obtained by the solicitor providing the advice. Text containing or commenting upon legal opinion or strategy cannot be sent to third parties except as expressly directed by Municipal Council or as required by law;
- Email and other messaging systems cannot be used to send any material which is obscene/pornographic (including sexually explicit material, full or partial nudity, sexually explicit jokes, sexually degrading material); racially offensive/degrading, defamatory; discriminatory; hate propaganda; harassing, threatening, or otherwise inappropriate as determined by the Corporation;

- Employees are prohibited from monitoring, intercepting, or tampering with another employee’s email or other messaging system communication except as authorized by this Procedure.

4.11. Procedure Violation:

A violation of this Procedure will result in corrective and/or disciplinary action. Such action may include, but is not limited to, an apology, coaching or counselling, education or training, warning, suspension or leave without pay, demotion, transfer, or termination of employment.

In all cases, the Director, People Services or designate and/or the Director, Information Technology Services or designate will investigate any alleged violations of the Policy. Interim measures, including, but not limited to, deactivating, or limiting a user’s account may be taken pending an investigation. Where a violation is substantiated, any corrective and/or disciplinary action taken will be placed in the employee’s personnel file.

Notes: This Procedure replaces the former “Computer Usage Policy”.