CITY OF VANCOUVER

CORPORATE POLICY

POLICY TITLE	Technology Acceptable Use
CATEGORY	Administrative
POLICY NUMBER	ADMIN-035
POLICY OWNER	Chief Technology Officer, Technology Services
ACCESS	Public

PURPOSE

This policy establishes the requirements for all Users when accessing Technology Assets. This policy should be read and understood by the User prior to use of any Technology Assets.

SCOPE

This policy applies to the use of all Technology Assets regardless of physical location.

DEFINITIONS

FIPPA means the *Freedom of Information and Protection of Privacy Act* (British Columbia).

Technology Assets means all data, networks, systems, computing and telecommunications devices owned, leased or used by the City and used or made available for use to Users.

User means any person accessing or using any Technology Assets.

POLICY STATEMENTS

1. **General use**
   Technology Assets are valuable resources provided to Users along with access to critical data and City networks to enable City business. Users are permitted to access Technology Assets only for purposes for which they have authorized permission, and only for activities that are responsible, safe, legal, ethical, and consistent with employee's duties, applicable laws and regulations and the City's Code of Conduct.

2. **Compliance**
   Users must be aware of applicable laws and regulations, licences, and terms of use that they enter into when using applications and websites and ensure that there are no conflicts with City policies. If Users have any questions regarding which websites and applications they are permitted to use, and under what terms of use, they can ask the ServiceDesk.

   Users are prohibited from copying or distributing copyrighted material, unless they have legal authorization to do so.

3. **Personal use**
   Personal use of Technology Assets by Users is a privilege that can be withdrawn at any time. Occasional personal use of Technology Assets is permissible provided that such use is compliant with the conditions of use in Section 1 above, does not cause any additional expense to the City, and does not negatively impact productivity or operations.

   Due to impact on capacity and cost, Users are not permitted to download, save or store videos, games or any personal files on Technology Assets. The City is not responsible for the loss of any personal files stored on Technology Assets and will not reimburse Users for any costs related to using personal technology, or home Internet service, to access City technology services.

4. **Using personal devices for City work**
   Occasional use of personal devices for City work is permissible if Users have not been assigned portable Technology Assets and work remotely. Such use must be compliant with the conditions of use in Section 1 above, and must not cause any additional expense to the City or negatively impact productivity or operations. Technology Services is resourced to effectively provide support for the use of Technology Assets only, and accordingly will prioritize support for Technology Assets and may refuse to support use of personal devices for City work when necessary.

5. **Public records**
   Users acknowledge that all records, including emails, resulting from personal or business use of Technology Assets can be requested by the public under FIPPA and disclosed in accordance with the provisions of this law. Information stored on, or accessed from, Technology Assets may be accessed by the City without notice for regular business, security, FIPPA or audit purposes.

6. **Users responsibility**
   Users are individually responsible for acceptable use and care of all Technology Assets assigned to them. Acceptable use and care includes:

   6.1 Permitted Users
   Users must login to Technology Assets using their assigned ID and password. They are the only User permitted to login, or use the device, while signed on with those credentials.

   6.2 Handling of Information
   In accordance with the City's Code of Conduct, City information that Users access, whether verbal, written, or electronic, must be safeguarded in a manner that ensures its confidentiality. Users must not share any information that puts the City at risk (e.g. server names, configuration settings, passwords, IP addresses, etc.) with unauthorized personnel.

   6.3 Protection of Privacy
   In accordance with the City's Privacy Policy, users that have access to Technology Assets must adhere to the privacy requirements consistent with their access. Users must also respect the privacy rights of other Users, not accessing or copying another User's email, data, programs or files without authorization.

6.4 Protected passwords

All Technology Assets must be passcode/password protected when not in use, and set to lock after a period of inactivity. Employee passwords are confidential and not to be shared with anyone. Passwords must not be communicated via email or written down.

6.5 Clean spaces

Desks not in use must be cleared of documents containing City business. Sensitive information such as passwords must never be available on a desk or device (e.g. post-it notes.) Documents in printers and meeting rooms must be removed after use.

6.6 Storing and sharing

When collecting, storing and sharing City information, Users must only use City-approved Technology Assets. Cloud storage solutions that are not City-approved are prohibited.

Portable data storage devices (such as USB keys) must meet the City standard for passwords and encryption, before being used.

Users must be especially cautious when sharing information or sending attachments to non-City e-mails. E-mail attachments are not secure and should not be used for confidential or personal data. Contact the ServiceDesk for alternative options.

6.7 Prohibited applications and subscriptions

All applications must be authorized and installed by Technology Services and meet the City's applicable standards, which are published through the ServiceNow service catalog. Users are not permitted to use cloud software and web applications that are not approved by Technology Services.

6.8 Responsible Internet usage

The City's Social Media Policy outlines the requirements for Users engaging on social media platforms. Internet usage must comply with Code of Conduct.

6.9 City e-mail is for City business

City e-mail is provided for City use. City e-mail must not be used for conducting Union business when acting as a Union representative. (e.g. Shop steward.) City e-mail must not be used for personal correspondence or for signing up for personal social media account or non-authorized web services. Users must not forward City e-mails to an outside e-mail address or use non-city e-mail accounts for conducting City business.

6.10 Remote access

Users must use an approved connection method (e.g. VPN) when connecting remotely to protect the City's information. Privileges and approved access may be provided to Users and third parties to enable access to City systems from outside of the physical network.

Throughout City locations, Technology Assets are available for shared use. From networked printers, to workstations at "hotel desks", to training rooms, Users should access and care for shared resources as if they were individually assigned to them.

6.11 Job changes

When Users change positions their Manager must notify Technology Services to adjust their access accordingly. The User must return any Technology Assets to Technology Services and request new Technology Assets to match their new role. Users may request to have assigned Technology Assets transferred with them if the request is appropriate and has approval of both former and new managers.

Users must not exchange devices with one another or repurpose a device without approval from Technology Services. Failure to follow process creates a risk for unauthorized access to sensitive information and Interferes with the management, accounting and control of Technology Assets.

6.12 Off boarding

When Users resign from the City, their manager is responsible to notify Technology Services and follow departure procedures. If departing Users have any administrative accounts or are subscribing to any online services on behalf of the City, their manager is responsible to work with Technology Services to securely off-board these services and accounts.

6.13 Buy outs

Users are not permitted to buy or keep Technology Assets when no longer employed by the City. Departing Users are not permitted to retain City phone numbers for personal use after leaving the City. Exceptions may be granted if Users obtain approval from both the Chief Technology Officer and General Manager and take responsibility for all associated costs.

7. Technology stewardship

Technology Services is responsible for addressing the technology needs of Users across the City by selecting and configuring Technology Assets; applying policies; developing standards; balancing security and usability requirements; and raising awareness for best practices.
These include:

7.1 Technology support

Technology Services provides ongoing support to City Users using devices that were issued by Technology Services and meet City standards through multiple channels including in-person support at City locations and remote support to other locations. Technology Services determines whether to troubleshoot, repair, upgrade, or replace, as needed. Users can request support from Technology Services through the ServiceDesk.

7.2 Limits to e-mail and messaging services

The City provides tools for communication including e-mail services, message services, VOIP softphones, faxing, and audio/video conferencing services. These services can be restricted, limited, or expanded anytime, without notice, to ensure business continuity.

7.3 Providing access to City Information
Information is owned by the City, and when necessary, with the appropriate approval(s),Technology Services may provide temporary access to City information such as e-mails, devices or network drive files to ensure business continuity or to support investigations related to violations of City policies.

7.4 Asset management
Technology Services may enable device and asset management systems for Technology Assets. This can include updating systems and applications, configuration settings, tracking location and locking down or wiping, as required, to maintain security and integrity.

7.5 Location tracking limits
The City will not utilize the location tracking capability of any systems to track the real-time or last-known physical location of a City device for generalized or random monitoring of employee performance. Technology Services may utilize these capabilities and associated data to secure a lost or stolen device; in the case of an emergency, to support an investigation; and, to evaluate the delivery and quality of our programs and services.

8. Exemptions
The City's Chief Technology Officer (or a Director with express written authority delegated to them by the City's Chief Technology Officer) may grant standing or single instance exemption to this policy where a valid business or security reason exists. Exceptions will be tracked and reviewed annually.

9. Violations
Any violation of this policy may result in disciplinary action up to and including termination.

10. References
This policy must be read and applied in conjunction with the City's following related corporate policies: Cybersecurity (ADMIN-36), Network Connectivity (ADMIN-37), Enterprise Data (ADMIN-38), Technology Lifecycle (ADMIN- 39), Privacy (ADMIN-029), Remote Work (ADMIN-047) and Technology Third Party Access (ADMIN-40).

APPROVAL AND REVIEW HISTORY:

Version 1 approved by:	Information Technology Security	1/24/2003
	Corporate Management Team (CMT)	1/24/2003
Version 2 approved by:	Information Technology Security	12/1/2004
	Corporate Management Team (CMT)	12/1/2004
Version 3 approved by:	IT Security – Risk Management / Office of the CTO	12/15/2016
	City Manager	12/15/2016
Version 4 approved by:	Director, Enterprise Technology	9/15/2020
	Chief Technology Officer	12/14/2020
	City Manager	12/24/2020
Version 5 approved by:	Director, Enterprise Technology	11/28/2022
	Chief Technology Officer	4/1/2023

Next review date: January 4, 2025