CORPORATE POLICY AND PROCEDURE

Policy:	**Technology Use Policy**
Coverage:	**Users of City Technology**
Issuing Department:	**IT & GIS**
Approved By:	**Executive Council**

Issued	Last Reviewed	Next Review
2019-12-16	2019-12-16	2020-11-01

Policy Statement

The technology use policy IT-2019-01 is a comprehensive policy document that is intended to provide guidance for any employee using City of Quinte West technology or employees who are overseeing the use of technology by contractors or guests. It is the employee's responsibility to apply this policy to any situation where it is applicable. This policy supersedes all existing known (see above) and unknown IT policies for the City of Quinte West.

The City of Quinte West recognizes the value of technology to provide tools to employees delivering their day to day functions. To this end, the City of Quinte West encourages the responsible use of technology and networks, including but not limited to the Internet, and other electronic resources in support of the mission and goals of the City of Quinte West and its affiliated user groups.

Because the Internet is an unregulated environment, information available to staff and guests is impossible to fully control. Therefore, the City of Quinte West adopts this policy, governing the use of technology and the Internet in order to provide guidance to individuals and groups obtaining access to these resources by any means.

The goal of this policy is to protect the integrity of all data that resides within the City’s technology infrastructure. The intention of this policy is to prevent data from being deliberately or inadvertently stored insecurely on any device or system where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the City’s public image. Therefore, all users employing any City device or service connected to any network used to backup, store, and otherwise access corporate data of any type must adhere to defined processes for doing so.

It is the policy of the City of Quinte West to maintain an environment that promotes ethical and responsible conduct in all online network activities by all users to include, but not limited to staff, guests and contractors. It shall be a violation of this policy for any employee, guest, or other individual to engage in any activity that does not conform to the established purpose and general rules and policies laid out in this document.

Enforcement

Employees shall comply with all policies and procedures contained in this policy, shall not deliberately violate the policy, and shall not knowingly or carelessly permit any unauthorized persons to use City of Quinte West systems or services or violate this policy. Employee conduct and the conduct of other persons permitted by employees can potentially have the City of Quinte West held liable and/or incur losses relating to the same, in which case costs and damages shall be required to be paid by the employee.

The IT team will notify an employee's manager of any violation of this policy immediately or as soon as practically possible. Any employee found to have violated this policy may be subject to disciplinary action up to and including termination at the discretion of management.

Navigation

This document is broken down into 5 sections:

- *Statements of each policy sub-section.*
- *The summarized purpose of each policy sub-section.*
- *Definitions.*
- *Governance and responsibilities of the City of Quinte West and Employees*
- *Revision history*

** Employees are responsible for reading and understanding the entirety of this document. Where indicated this policy highlights **EMPLOYEE RESPONSIBILITIES** to better help with this requirement, however, it is not meant to remove the requirement for understanding the rest of the document and does not limit the application of **ALL** sections to employees.

This policy replaces policies:

- IT-01 - Acceptable Use of Technology
- IT-02 - Password Policy
- IT-03 - Remote Access
- IT-04 - Third Party Access
- IT-05 - Anti-Virus Policy
- IT-06 - Mobile Device Policy
- IT-07 - Data Protection

Document Owner: Director, Corporate Services
Document Contact: Manager, Information Technology & GIS Services

Policy Statements

Policy statements are descriptions of what each subsection of the policy will address.

1. Acceptable Use of Technology
   - This policy outlines the general acceptable use of technology at the City of Quinte West.

2. Mobile Devices
   - This policy outlines the requirements regarding acceptable usage of mobile devices.

3. Email, File Storage & Collaboration Tools
   - This policy outlines the requirements regarding acceptable use of City email and collaboration suite system. (Google G Suite)

4. Passwords & Security
   - This policy outlines the requirements regarding passwords and security best practices for City systems.
   - This policy outlines the use of anti-virus systems on City of Quinte West devices and systems.

5. Guest WiFi & Third Party Access
   - This policy outlines the responsibilities regarding guest access to City WiFi systems.
   - This policy outlines the responsibilities regarding third party (contractor / consultant / supporting company) access to City of Quinte West systems and/or infrastructure.

6. Video Surveillance
   - This policy describes the use of video surveillance throughout the City of Quinte West.

7. Telephony Best Practices
   - This policy describes best practices around mobile and desktop phone system use.

8. SaaS (Software as a Service) & Cloud Computing
   - This policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.
   - This policy describes best practices around the adoption of SaaS or cloud computing technologies.

Purpose Summaries

1. The purpose of the acceptable use of technology policy is to:

    1.1. Provide a clear understanding of the general responsibilities of employees.
    1.2. Provide a clear understanding with respect to the general acceptable use of technology at the City of Quinte West.

2. The purpose of the mobile device policy is to:

    2.1. Provide an understanding of expectations of privacy and use of devices.
    2.2. Provide a uniform approach for the distribution of mobile devices to employees.
    2.3. Provide a uniform approach for the method of returning mobile devices.
    2.4. Provide policy around travelling with mobile devices.
    2.5. Provide policy around use while operating a motor vehicle or other mechanical or motorized equipment.
    2.6. Provide policy around damage or loss of devices.
    2.7. Provide policy around the use of shared devices.
    2.8. Provide policy around data usage on cellular enabled devices.
    2.9. Provide policy around the personal use of mobile devices.
    2.10. Provide policy around BYOD (Bring Your Own Device).

3. The purpose of the email and collaboration tools policy is to:

    3.1. Provide a clear understanding around expectations of privacy.
    3.2. Provide a comprehensive understanding around data loss prevention and the handling of sensitive information.
    3.3. Provide guidelines around the use of Email.
    3.4. Provide guidelines around the use of Google Drive.
    3.5. Provide guidelines around the use of Calendar.
    3.6. Provide clear understanding and policy with respect to copyrighted content.

4. The purpose of the passwords and security policy is to:

    4.1. Provide a clear understanding regarding the expectation of password complexity.
    4.2. Provide a clear understanding regarding password reuse.
    4.3. Provide a clear understanding regarding password change frequency.
    4.4. Provide a clear understanding around password care and use.
    4.5. Provide a clear understanding of building access cards and devices.

4.6. Provide a clear understanding with respect to locking applicable devices.
4.7. Provide a framework around the use of portable writeable media such as USB removable media and memory cards.
4.8. Provide a clear understanding around the use of anti-virus systems for the protection of City systems and devices.
4.9. Provide policy and understanding around phishing.

5. The purpose of the Guest WiFi & Third Party Access policy is to:

5.1. Provide a clear understanding of guest WiFi access.
5.2. Provide a clear understanding with respect to third party access to City of Quinte West systems and/or infrastructure.

6. The purpose of the video surveillance policy is to:

6.1. Provide policy around expectations of privacy.
6.2. Provide a clear understanding of how the City of Quinte West uses video surveillance throughout municipal buildings and infrastructure.
6.3. Provide a clear understanding of how to request CCTV recordings.

7. The purpose of the telephony best practices policy is to:

7.1. Provide a clear understanding around voicemail.
7.2. Provide a clear understanding with respect to best practices using mobile phones and desktop phones and accessories.

8. The purpose of the SaaS & Cloud Computing policy is to:

8.1. Provide clear guidelines around the general use of SaaS and cloud computing technologies and services at the City of Quinte West.
8.2. Provide a clear understanding around the use of personal cloud accounts.

Appendix A: Revision History

Definitions

EMPLOYEE RESPONSIBILITY:
It is the employee's responsibility to read and understand all definitions in this category.

- **2FA / MFA**
    - 2FA is Two Factor Authentication
        - Passwords are information the user *knows*. 2FA is a method of confirming the users claimed identity by using a combination of *something they know* with *something they have* or *something they are.* For example, a password (something you know) combined with a one-time token (something you have) provides two factors of authentication.
    - MFA is Multi Factor Authentication
        - Similar to 2FA, MFA is proving identity through two or more factors.

- The City of Quinte West defines **acceptable business use** as activities that directly or indirectly supports the business of The City of Quinte West.

- The City of Quinte West defines **acceptable personal use** as reasonable personal communication or recreation, such as reading or game playing.

- **Anti-Virus** is software designed to detect and destroy computer viruses.

- **Application Programming Interfaces (APIs)** are standard contracts that define how developers communicate with a service, and the kind of output those developers should expect to receive back. APIs are typically used by a program to communicate to a service and get an expected output.

- A **browser plugin** is software which adds functionality to a web browser, and is often developed by a third-party.

- **Biometric security** is a security mechanism used to authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics. Fingerprint identification is an example of a biometric identification mechanism.

- **BYOD** - Bring Your Own Device

- **CCTV** (closed-circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. **CCTV** relies on strategic placement of cameras, and observation of the camera's input on monitors somewhere.

- **Cellular provider** is a company that provides cellular service to cell phone users.

- Similar to a browser plugin, a **Chrome extension** adds functionality to the web browser. The difference between a Chrome plugin and a browser plugin is that a Chrome plugin modifies core functionality of the browser to add more extensive functionality.

- **City / The City**: The Corporation of the City of Quinte West.

- A **City Owned Device** is any device or technology that the City of Quinte West has provided a staff member, contractor, member of council, or any other person or organization.

- A **computer virus** is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a **computer virus**.

- **Content -** Any information that is communicated on a social media channel.

- **Copyright** is a law that gives the owner of a work (for example, a book, movie, picture, song or website) the right to say how other people can use it. **Copyright** laws make it easier for authors to make money by selling their works. ... With **copyright**, a work can only be copied if the owner gives permission.

- The unauthorized transfer of classified information from a computer or datacentre to the outside world. **Data leakage** can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by remote removal through local networks or the internet.

- **Data loss prevention (DLP)** is a strategy for making sure that users do not send sensitive or critical information outside corporate infrastructure. It is the responsibility of the user to ensure that corporate data is not shared, or otherwise distributed unless deemed necessary for work functions.

- **Data retention**, also called records retention, is the continued storage of an organization's data for legal or business reasons or to comply with data archival regulations. When the retention time of a specific set of data has expired, it either gets moved to a tertiary storage as historical data or gets deleted entirely to keep storage spaces clean.

- A **denial-of-service** attack is a security event that occurs when an attacker prevents legitimate users from accessing specific computer systems, devices, services or other IT resources. Denial-of-service

(DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them.

- The **Device Policy** is the app enforces your organization's security policies on your device to protect corporate data and make it more secure. If you don't install the app, but your admin requires it, you can not access G Suite data on your device, including work email, calendar, and contacts.

- **Downloading** is the transmission of a file or data from one computer system to another. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.

- **Electronic Funds Transfer (EFT)** is a system of transferring money from one bank account directly to another without any paper money changing hands. One of the most widely-used EFT programs is direct deposit, through which payroll is deposited straight into an employee's bank account. However, EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, and point-of-sale (POS) transactions. It is used for both credit transfers, such as payroll payments and for debit transfers, such as mortgage payments.

- **Employees** are considered any individual working for the City. Including regular full time, part time, contract, contractors, casual, seasonal and consultants. Employees can also include Mayor and Council with respect to this policy.

- Data **encryption** translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. **Encrypted** data is commonly referred to as **ciphertext**, while unencrypted data is called **plaintext**.

- An **executable** file is a type of computer file that runs a program when it is opened. This means it executes code or a series of instructions contained in the file.

- A **firewall** is software that enforces a set of rules about what data will be allowed to enter or leave a computer network. A firewall's main purpose is to filter traffic and lower the risk that malicious packets traveling over the public internet will be able to impact the security of a private network. Firewalls can also restrict internal traffic to resources based on access control rules.

- **Identity as a Service (IDaaS)** is an authentication infrastructure that is built, hosted and managed by a third-party service provider. IDaaS can be thought of as single sign-on (SSO) for the cloud.

- To **indemnify someone** is to absolve that person from responsibility for damage or loss arising from a transaction. **Indemnification** is the act of not being held liable for or being protected from harm, loss, or damages, by shifting the liability to another party.

- **Infrastructure as a service (IaaS)** is a form of cloud computing that provides virtualized computing resources over the internet. IaaS is one of the three main categories of cloud computing services, alongside software as a service (SaaS) and platform as a service (PaaS).

- **Insecure WiFi** networks are those which are secured with WEP (wired equivalent privacy) security. These are not to be used.

- The **Internet**: an electronic communications network that connects computer networks and organizational computer facilities around the world.

- **Malware** is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

- A **mobile device** is identified as any technology which accesses City systems that is portable and can be used both inside and outside physical City locations and networks. Example mobile devices include but are not limited to:

    - Laptops
    - Chromebooks
    - Tablets
    - Cellular Phones - both smart and otherwise
    - Pagers

- **Negligence** is determined to be a failure to take proper care in doing something or caring for physical property.

- A **network**, in computing, is two or more devices or computer systems connected by physical and/or wireless connections which enable them to communicate. This can range from a single PC connected to basic peripherals to massive data centers located around the world, to the Internet itself. Regardless of scope, all networks allow computers and/or individuals to share information and resources.

- **Open WiFi** networks are WiFi networks without passwords.

- **PDF**: Portable Document Format. PDF is a file format designed to present documents consistently across multiple devices and platforms. It was developed by Adobe 1992 and has since become one of the most widely used formats for saving and exchanging documents.
  A PDF file can store a wide variety of data, including formatted text, vector graphics, and raster images. It also contains page layout information, which defines the location of each item on the page, as well as the size and shape of the pages in the document. This information is all saved in a standard format, so the document looks the same, no matter what device or program is used to open it. For example, if you save a PDF on a Mac, it will appear the same way in Windows, Android, and iOS.
  The PDF format also supports metadata, such as the document title, author, subject, and keywords. It can store embedded fonts so you do not need to have the appropriate fonts installed to view the document correctly. PDF documents may also be encrypted so only authorized users can open them.

- **Personally identifiable information (PII)** is any data that, when used alone or with other relevant data, could potentially identify a specific individual. Such information includes biometric information, medical information, financial information and unique identifiers such as passport or Social Insurance Numbers (SIN).

- **Phishing** is the fraudulent practice of sending emails or other communication purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

- **Platform as a service (PaaS)** is a cloud computing model in which a third-party provider delivers hardware and software tools - usually those needed for application development - to users over the internet. A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.

- **Piracy** is using the Internet to illegally copy and/or distribute software.

- **Portable Media**: (Some common portable media devices)
  - USB Devices
    - Jump drives
    - Thumb drives
    - Memory stick
  - Memory Cards
    - SD Card
    - Micro SD Card
  - Hard Drives
    - USB connected hard drives

- **Ransomware** is a type of malicious software designed to block access to a computer system until a sum of money is paid. This is usually accomplished using encryption.

- **Roaming** is using your data enabled mobile device on another service provider's network when travelling outside of Canada.

- **Rooting** is a process that allows you to attain root access to the Android operating system code (the equivalent term for Apple devices is **jailbreaking**). It gives you privileges to modify the software code on the device or install other software that the manufacturer wouldn't normally allow you to.

- **Software as a Service (SaaS)** is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).

- **Social Media** - Internet based websites and applications that enable the creation and sharing of content, or to participate in social networking.

- **Sponsoring a guest WiFi user** is the act of granting a user access to City of Quinte West guest WiFi by using the guest WiFi portal https://guestwifi.quintewest.io

- **Spyware** is software that is installed on a computing device without the end user's knowledge. Any software can be classified as spyware if it is downloaded without the user's authorization. Spyware is controversial because even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused.

- **Tailgating**: An employee opening and holding a door for another person without proper access or the passive acceptance of a uniformed worker. This could also happen without the knowledge of the employee accessing the area.

- **Tethering** is to use a data enabled mobile device (like a cellphone) as a mobile hotspot to connect another nearby device (like a laptop or tablet) to the Internet.

- In computing, a **Trojan horse** is any malware which misleads users of its true intent. They are generally spread by some form of social engineering, for example where a user is duped into clicking an e-mail attachment disguised to appear not suspicious, or by clicking on a fake advertisement on social media or anywhere else. Although their payload can be anything, many act as a backdoor, which can give unauthorized access to the affected computer. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network. Ransomware attacks are often carried out using a Trojan.

- **Unknown WiFi** networks are those which are not created or maintained by yourself, family or friends. Examples of this may include hotel or airport WiFi.

- A **virtual private network** (**VPN**) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Examples include encrypting traffic across open WiFi networks by connecting using **VPN** to City networks.

- A **web browser**, or simply "**browser**," is an application used to access and view websites. Common **web browsers** include Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

- **Wired Equivalent Privacy (WEP)** is a security protocol that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is easily crackable and not recommended.

- **WiFi** for the purpose of this document is any wireless access point/device capable of allowing access to a private network, the Internet or both.

- A computer **worm** is a standalone malicious software program (malware) that replicates itself and spreads to other connected computers with no human intervention. Worms use parts of an operating system that are automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. USB drives are a common vector for computer worms.

- **WiFi Protected Access (WPA)** is a security standard for wireless network connections. WPA was developed to provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP), the original Wi-Fi security standard.

Governance & Responsibilities

1. Acceptable Use of Technology

1.1. General Responsibilities

1.1.1. Employees are responsible for:

1.1.1.1. Adhere to the terms and conditions of this policy and be aware of the consequences when in contravention. Depending on the severity of a violation, employees may be subject to disciplinary action up to and including termination.
1.1.1.2. Ask questions if any of the content of this policy is not understood.
1.1.1.3. Familiarize themselves with this policy and adhere to its requirements.
1.1.1.4. Never leave technology unattended, especially in a logged in state.
1.1.1.5. Take all reasonable steps to protect the security and maintenance of the equipment by promptly reporting any damage, theft, or vandalism to the IT department.

1.1.2. Managers / Supervisors are responsible for:

1.1.2.1. Reviewing data usage billing for employees who report to them.
1.1.2.2. Responding to inappropriate use of technology and equipment.
1.1.2.3. Supporting the consistent application and promoting awareness of this policy.

1.1.3. Directors are responsible for:

1.1.3.1. Reviewing data usage billing for employees who report to them.
1.1.3.2. Responding to inappropriate use of technology and equipment.
1.1.3.3. Supporting the consistent application and promoting awareness of this policy.
1.1.3.4. Conducting investigations with respect to violations of this policy.

1.1.4. IT is responsible for:

1.1.4.1. Providing a safe and secure technology environment for the purpose of conducting the business of the City of Quinte West.
1.1.4.2. Provide recommendations to any employee or department who requires guidance in the appropriate application or acquisition of technology.
1.1.4.3. Providing support for investigations into violations of this policy.
1.1.4.4. Responding to inappropriate use of technology and equipment.

1.1.4.5. Supporting the consistent application of this policy.

1.1.5. Directors and HR representatives retain the right to report any illegal violations to the appropriate authorities with or without the knowledge of the offending individual.

1.2. General Acceptable Use

1.2.1. The IT team attempts to block the installation and use of software and/or services that may put City technology and/or data at risk. There is no ability to ensure that this is 100% effective at blocking all possible risks.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to limit the adoption of any service (SaaS software as a service) or the installation of any software, plugins, extensions or otherwise that may cause the compromise of City systems. When in doubt it is the responsibility of the employee to contact the IT team to ensure safe usage.*

1.2.2. All information created by or with the City of Quinte West's technology and/or services are records for the purposes of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Freedom of Information and Protection of Privacy Act, and other related legislation and regulations and may be a public record for the purposes of the legislation.

1.2.3. The corporate records management policy applies to all information stored on City infrastructure and services and to City owned devices.

1.2.4. Where any policy of the City of Quinte West contradicts this policy the more conservative or restrictive policy shall be followed.

1.2.5. All information stored on City technology and services is considered a corporate record and there is NO guarantee that personal information will remain private. Therefore, it is prohibited to store personal information on corporate infrastructure or services. Accessing personal information through accounts, such as a personal Google account, is allowable providing that no information is stored locally on the device. This includes accessing a personal album of photos in a service such as Google Photos.

1.2.6. No records of the City of Quinte West are to be stored on systems located at private residences or systems not under the control of the City of Quinte West.

1.2.7. Unauthorized repair or modification of any technology asset is prohibited.

1.2.8. Network devices are prohibited from being connected to City networks by employees. If connection is required the IT team suggests using the guest WiFi access. This especially refers to any networking devices that routes traffic. (ie. a Linksys router)

1.2.9. Any technology use must not violate federal, provincial or local laws or the City's Code of Conduct.

1.2.10. Any technology use must not circumvent the City's firewall.

1.2.11. Employees shall not browse any website which contains materials that are reasonably considered offensive, obscene, pornographic or hateful. Unless specifically required for work purposes.

1.2.12. Employees shall not copy or reproduce in any form, any software. Employees shall not use City systems or facilities to copy or reproduce in any form, any software or copyrighted materials. Piracy is prohibited.

1.2.13. The access of another user's account with or without consent unless directed to do so by the office of the CAO, or designate, is prohibited.

1.2.14. An individual's user account will only be accessed by that individual. Sharing of accounts and passwords is prohibited. Shared accounts can be requested if the need exists.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure the privacy of their individual accounts by not sharing their passwords with anyone.*

1.2.15. The installation of software licensed to the City on any technology resource not owned or provided by the City is prohibited.

1.2.16. The City of Quinte West reserves the right to monitor all corporate assets to determine violations of this policy. Access to technology, systems and data from active or former employees and elected officials without the user's consent for the purposes of enforcing this policy is permitted.

1.2.17. All technology equipment acquired through the IT department is property of the City of Quinte West.

1.2.18. The IT department is not responsible for the support of any personal technology assets located at private residences of employees or members of council. Physical support will be conducted on City property only. City assets may be supported remotely by IT staff if deemed necessary by the technician.

1.2.19. The City is not responsible for personal misuse of corporate technology, equipment or services. In addition to discipline measures up to and including termination, persons found to be intentionally misusing the City's technology, equipment or services will be responsible for any and all costs or damages sustained by the City or a third party and will be obligated to indemnify the City for any claim against the City by a third party.

2. Mobile Devices

2.1. Use and Expectations of Privacy

2.1.1. This policy applies to any device that could be used to access City systems, even if the device is not corporately, owned or supplied (BYOD - Bring Your Own Device).

2.1.2. All devices (including BYOD) can be requested, if used for City business of any kind, and must be provided by the employee in the event of an FOI (freedom of information) - MFIPPA or FIPPA request.

2.1.3. Employees using devices owned by the City of Quinte West or devices that access City of Quinte West systems have NO expectation of privacy on any of these devices.

2.1.4. All communication (email, SMS, MMS, hangouts, photos etc.), and storage including cloud and on site or on device is considered property of the City of Quinte West. This information can be accessed and/or requested by IT or management at anytime and released through a Freedom of Information request or for investigation of possible breaches and/or misuse. Employees agree to and accept that their access and/or connection to any network may be monitored.

2.1.5. Any communications sent from mobile devices will not contain any offensive, obscene, defamatory or harassing messages. Messages intended to annoy, or intimidate another person are strictly prohibited and would be in violation of the City's Code of Conduct.

2.1.6. The IT department is not responsible for conflicts that arise from the use of software, or services not installed and supported by the IT team.

2.1.7. At **all times** the browsing, storing or viewing of illicit materials, including but not limited to pornographic content, is prohibited on City owned devices.

2.1.8. The IT department reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to any networks or infrastructure. IT will engage in such action if it feels such equipment is being used in a way that puts the City's systems, data, users and clients at risk.

2.1.9. Passwords must secure all mobile devices.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to ensure that mobile devices are secured using an acceptable password. It is important that the default password is changed when the employee receives the device.*

2.1.10. Mobile devices must not be modified in any way, this includes, but is not limited to rooting and jailbreaking devices.

2.1.11. Any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company information must be immediately reported to the IT team.

2.1.12. Mobile devices should be physically secure at all times.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to ensure the physical security of all mobile devices at all times, while in use or not in use.*

2.2. Distribution of Mobile Devices

2.2.1. All devices distributed by the IT team are the property of the City of Quinte West.

2.2.2. All devices are not to be lent to other employees, family or friends.

2.2.3. All devices will be distributed with Quinte West asset tags.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to periodically check to ensure that the asset tag on their devices is present and in good condition. If it is not, the employee is to contact the IT department for a replacement.*

2.2.4. Mobile devices will be given to employees who are deemed required to use that device for their job function. Choice of mobile device is at the sole discretion of the IT department and department director.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to request a mobile device through their manager if needed and they do not have one.*

2.2.5. Accessories:

- Some mobile devices will be distributed with a protective case to ensure that reasonable handling of the device will not damage it.
- Mobile devices will be distributed with 2 charging cables for use where the employee sees appropriate.

EMPLOYEE RESPONSIBILITY: *It is the employee’s responsibility to ensure that all necessary items are with the mobile device before accepting delivery.*

EMPLOYEE RESPONSIBILITY: *If the mobile device did not come with a case, such as the case with laptops, care should be taken when transporting these devices so they do not become damaged.*

2.3. Return of Mobile Devices

2.3.1. Mobile devices are to be returned to the IT department upon the following conditions:

- Damage
- Change in position that no longer requires the use of a mobile device
- Termination of employment

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to return mobile devices clean and in working order upon the need to return the item. All accessories are to be returned with the mobile device as well.*

Passwords or any other method that secures access to the device must be provided so the IT Team can access the device. It would be good practice to change that password or pin to a value that is not used in any other of your systems or sites.

2.3.2. Requests to take your mobile number when retiring may be approved upon the following conditions and is subject to approval by the CAO or designate:

- The number is not required by the City
- The employee is willing to pay any early cancellation fees

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to notify IT staff in writing, if they are interested in retaining their mobile number several weeks prior to their last day of work. IT Staff will contact the cellular provider to determine the amount (if any) of the early cancellation fee.*

EMPLOYEE RESPONSIBILITY: *Once permission for a "Transfer of Responsibility" has been noted on the account, it is the responsibility of the employee to contact the cellular provider to request their number be moved to a personal plan, which may include a credit check on the employee. This must be completed in a timely manner, or the City has the right to refuse the transfer.*

2.3.3. Disposal: The IT department will evaluate and either dispose of the item in an environmentally responsible way or re-purpose the device back into the technology pool.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to return any malfunctioning or broken mobile devices to the IT department and not throw it out of their own accord.*

2.4. Travelling with mobile devices.

2.4.1. Travelling with mobile devices is permitted by the City of Quinte West. If no care is taken, these activities can incur extra costs if not used in a responsible manner.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that all sections of this policy are followed when travelling with mobile devices.*

2.4.2. The IT team will ensure that all precautions are taken to mitigate large charges due to travel and roaming. This includes any necessary training with respect to the functions of your mobile device.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to learn and understand all functions of their device to help in the mitigation of large usage charges. ANY and ALL costs that are incurred are, at the discretion of their director, are the SOLE responsibility of the employee.*

2.4.3. Cellular mobile devices are permitted to be used throughout Canada. If travelling outside of Canada roaming data must be turned off and that secure WiFi is used exclusively. Alternatively a travel SIM (Subscriber Identity Module) card can be used. Exceptions can be made at the discretion of the director.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to learn and understand the operation of the cellular mobile device to ensure that costs are not incurred due to roaming data, voice or text while travelling.*

2.4.4. The use of a travel (employee provided) SIM card in your cellular connected device is permitted when travelling outside Canada, and is suggested if you wish to use your phone for personal use while roaming, to ensure that extra costs are not incurred by the City.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that while travelling outside of Canada any actions that may incur cost are done for work purposes only.*

2.4.5. The City will provide a paid roaming plan for the employee, if it is determined by their manager, that they need to be connected or available while travelling outside of Canada.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to inform the IT team when and in which countries they will be travelling when leaving Canada with their cellular enabled mobile device. This notice should be submitted VIA the helpdesk at least 2 weeks prior to departure so that the IT team can provision the correct plan for the phone and give any education necessary with respect to the proper operation of their mobile device abroad.*

2.4.6. Cellular usage is strictly prohibited on any foreign waters including while travelling on cruise ships to prevent excessive roaming charges by 3rd party cellular providers.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to arrange for alternate methods of communication, at their own expense, if required.*

2.4.7. The use of unknown, insecure or open WiFi networks is prohibited without the use of a Virtual Private Network (VPN). If this is in question, the IT team recommends using cellular data to connect to resources. Your home WiFi network and the WiFi networks of friends and family are not generally considered to be insecure.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to be able to identify an open, insecure or unknown WiFi network.*

2.4.8. A VPN service can be requested if required, and approved by a manager.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to submit a request VIA the Helpdesk to set up a VPN on mobile device prior to travelling.*

2.4.9. Tethering is NOT permitted when travelling outside of Canada. It is at the discretion of the director to override this policy.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure they never use their mobile device as a wireless hotspot when travelling outside of Canada to mitigate large usage charges.*

2.5. Use while operating a motor vehicle or other mechanical or motorized equipment .

2.5.1. The use of a handheld device while in a motor vehicle must obey ALL laws and regulations. Bill 118 amends the Highway Traffic Act to expressly prohibit the holding or use of hand-held wireless communications and electronic entertainment devices, including cellular phones and smartphones. This law also prohibits the presence of a television, computer or other device with a display screen if the display screen is visible to the driver (navigation devices such as GPS are permissible). All City of Quinte West employees are required to comply with this law. Employees who violate this are engaging in prohibited conduct for which they may be personally liable at law should damages result from misconduct.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to know, understand and follow all of these regulations.*

2.5.2. Individuals are strictly prohibited from making or receiving calls on a cellular telephone or mobile device while operating a motor vehicle. This includes both City issued and personal cellular telephone and mobile devices.

2.5.3. The IT team will provide assistance and equipment to ensure that all laws and regulations with respect to operating a City owned motor vehicle are respected. The provisioning of this equipment is at the discretion of the manager. In the event the vehicle does not have hands-free capabilities the employee should not use their devices.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to request these services if required.*

2.5.4. Any violation of laws by an employee is in direct violation of this policy. Any fines incurred will be the responsibility of the employee.

2.5.5. Emergency Services employees are exempt from this section when performing their duties as approved by Emergency Services. Specific Policies for emergency workers can be obtained through the Ontario Highway Traffic Act.

2.5.6. Using any device while operating City equipment will follow the same laws and regulations as those while operating a motor vehicle. Such equipment includes, but is not limited to:

- Heavy equipment such as loaders, backhoes and excavators.
- Lawn mowers.
- Sidewalk plows.
- Handheld motorized devices such as chainsaws, trimmers and power tools.

2.6. Damage or Loss of Devices

EMPLOYEE RESPONSIBILITY:

THE EMPLOYEE IS SOLELY RESPONSIBLE FOR THE CARE AND OPERATION OF ANY DEVICE. ANY MISUSE, AS DEFINED BY VIOLATIONS OF THIS POLICY, OF THESE DEVICES BY ANYONE IS THE RESPONSIBILITY OF THE EMPLOYEE ASSIGNED THE DEVICE .

2.6.1. Lost or stolen devices must be reported to IT immediately. IT will attempt to remotely wipe the device of data and lock it. If the device is recovered it will be re-provisioned to the user.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that lost or stolen devices are reported to IT immediately.*

2.6.2. Damage or loss of devices caused by negligence will not be tolerated.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that the use of the device does not incur extra risk.*

2.6.3. Chronic damage or loss of devices is a direct violation of this policy.
Repercussions of chronic damage or loss will include but is not limited to:

- Wage garnishment.
- Loss of privilege.
- Disciplinary measures up to and including termination.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that chronic damage or loss does not happen. Chronic damage or loss is defined at the sole discretion of the IT department and will be discussed with the employees manager.*

2.6.4. The distribution of mobile devices will include necessary protective cases, bags or other items to ensure that regular use of technology will not damage the device.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to use all protective devices with their mobile device.*

2.6.5. Damage or loss will also extend to accessories of devices.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to take care of accessories provided with devices.*

2.7. Shared Devices

2.7.1. The IT department may deploy shared devices for the purposes of conducting City business. Shared devices include but are not limited to:

- Chromebooks in shared areas such as lunch rooms.
- Tablets in shared areas. (Time Tracking, Work Order System, etc.)
- Pagers

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that these shared devices are used in a responsible manner, taking into consideration all the sections of this policy.*

2.7.2. Shared devices will be checked for damage upon return and at regular intervals. Any damage to these devices caused by gross or intentional negligence will not be tolerated.

EMPLOYEE RESPONSIBILITY: *It is the sole responsibility of the employee to ensure that the use of these devices do not incur extra risk.*

2.7.3. Shared devices should only be used for their intended purpose.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that these devices are used for their intended purpose.*

2.7.4. The IT team will provide a means by which to report damage or misuse of shared equipment.

EMPLOYEE RESPONSIBILITY: *Upon use of these devices, any damage must be reported to the IT department VIA the helpdesk.*

2.8. Data Usage on Cellular Enabled Devices

2.8.1. Data usage on cellular enabled devices is enabled to ensure that business services can be accessed independently of City networks.

2.8.2. Data limit will be set by IT at **6GB**.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that cellular data usage does not exceed **6GB** of use.*

2.8.3. Data warning will be set by IT at 5GB.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that the cellular data warning setting is set at 5GB and to inform the IT team if the data warning is reached.*

2.8.4. Data tethering is permitted on City owned mobile devices within Canada only.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to make sure that all precautions and settings are enabled to ensure that tethering of mobile devices to other devices does not incur significant costs due to data overage or any other reason.*

2.9. Personal Use

2.9.1. Incidental personal use of mobile devices is permitted provided all sections of this policy are adhered to, the privilege is not abused and use does not interfere with City business.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that personal use of mobile devices is in accordance with this policy and does not interfere with City business.*

2.9.2. Connection to private ("home") WiFi networks is preferred to limit the amount of cellular data used by cellular enabled devices.

2.9.3. Expectations of use during personal time or non-work time for the purpose of conducting City business is to be discussed with the employees manager.

2.9.4. Individuals shall be responsible for financial reimbursement to the City of Quinte West for invoicing associated with the use of the cellular devices if personal use is not considered reasonable and incidental to the primary function of communication for work-related purposes. Such "reasonable use" shall be at the discretion of the department head.

2.9.5. With respect to cellular enabled mobile devices, specifically smartphones, the IT department does strongly suggest that the employee carry the phone during the working day even during breaks and lunches as there are some security and notification functions of the phone that can provide a greater level of personal safety throughout the day.

2.10. BYOD (Bring Your Own Device)

2.10.1. Employees are permitted to use personal devices to access City email and collaboration systems.

EMPLOYEE RESPONSIBILITY: *The employee is expected to use their devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.*

2.10.2. The City of Quinte West reserves the right to disconnect devices or disable services without notification.

2.10.3. Employees will be required to install the City device policy when adding these accounts to their personal devices to ensure protection of City intellectual property.

EMPLOYEE RESPONSIBILITY: *The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.*

2.10.4. Employees will not be compensated for any costs associated with the use of personal devices with City systems.

2.10.5. The employee's device may be remotely wiped if:

a. The device is lost.
b. The employee terminates their employment.
c. IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

EMPLOYEE RESPONSIBILITY: *While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc. on personal devices.*

3. Email, File Storage & Collaboration Tools

3.1. Expectation of Privacy

3.1.1. Employees have NO expectation of privacy with respect to City of Quinte West systems, devices and/or services.

3.1.2. All devices, software systems, email, chat, calendar and file storage can be searched and audited by authorized City of Quinte West employees both manually and automatically for breaches of this policy.

3.1.3. Personal use within the City of Quinte West systems is prohibited. All personal correspondence (email, chat, social media, etc.), appointments and file storage should be kept separate from City systems.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that no personal use of City systems is conducted. Personal use should be kept on services not provided by the City. One example would include a personal email address.*

3.2. Data Loss Prevention (DLP) & Sensitive Information

3.2.1. Data loss prevention (DLP) is a strategy for making sure that users do not send sensitive or critical information outside corporate infrastructure. It is the responsibility of the user to ensure that corporate data is not shared, or otherwise distributed unless deemed necessary for work functions.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that DLP practices are adhered to.*

3.2.2. Sharing of corporate data outside of corporate infrastructure should be done with care. The following is a non-exhaustive list of steps that should be taken to ensure compliance with this policy:

- Regularly review what documents and files are shared with external and internal users.
- Regularly review shared folder memberships to ensure that only the people who are necessary are shared on these resources.

- When sharing a file, take note of options to prevent download, print and copy of shared documents.
- Only share documents, files and folders with external individuals when absolutely necessary.
- As a best practice, put these shares in a dedicated place within your drive, so you can better audit these shares at later dates.
- Take note of access level (edit, view, comment) when sharing information and use the least level of access methodology when sharing.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that these suggestions are followed to limit the loss of City owned data.*

3.2.3. Sensitive information includes, but is not limited to:

- Social Insurance Numbers (SIN)
- Passport Numbers
- Passwords
- Personally identifiable financial information (ie. Credit Card Numbers, Bank Account Numbers)
- Biometric Data

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to understand what sensitive information is.*

3.2.4. Transmission of sensitive information: At all times sensitive information should NEVER be emailed or transmitted in any form of un-encrypted communication (if in question contact the IT department to ensure the method of communication is secure).

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to understand how sensitive information should be transmitted.*

3.2.5. Storing of sensitive information: When storing sensitive information it should be stored in an encrypted manner so that compromise of the system will not lead to a data leak.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to understand how to store sensitive information.*

3.3. Email

3.3.1. The IT department will provide access to an email system with unlimited storage for email and attachments to employees whose job function requires this access.

3.3.2. The IT department will provide a method to transfer email to another user or to historical records in the event that account is no longer needed.

EMPLOYEE RESPONSIBILITY: *If a transfer of a mailbox is required, it is the employee's responsibility to request this transfer and have it pre-approved by their manager.*

3.3.3. The IT department will provide a 3 times daily backup to the email environment with the ability for users to restore these backups at their discretion.

EMPLOYEE RESPONSIBILITY: *Employees are encouraged to self-serve recoveries of emails. Information on this system can be found on the help desk site.*

3.3.4. When sending email or any other type of communication employees represent the City of Quinte West and are expected to be professional and courteous.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee that they shall not:*

- *Misrepresent themselves or the City of Quinte West.*
- *Knowingly communicate any falsehood.*
- *Make any representations, undertake any obligation or incur any liability, beyond the employee's authority.*
- *Harass or intimidate any person.*
- *Transfer, post or otherwise communicate any materials that are reasonably considered offensive, obscene, pornographic, demeaning, hateful, defamatory, slanderous or libelous.*
- *Transfer, post or otherwise communicate or disclose any materials known by the employee to be, or that should reasonably be considered confidential, sensitive or proprietary to the City of Quinte West or to any person to whom the City may have confidentiality obligations.*
- *Transfer, post or otherwise communicate or disclose any materials that should reasonably be considered damaging to the City of Quinte West's reputation or other interests if disclosed.*

3.3.5. Email is to be used for City of Quinte West BUSINESS PURPOSES ONLY. A personal email account should be used for personal email.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that personal email is not stored on City systems. Employees can expect no level of privacy for any email stored on City systems.*

3.4. Google Drive

3.4.1. The IT department will provide access to a file storage area with unlimited storage capability to employees whose job function requires this access.

EMPLOYEE RESPONSIBILITY: *It is the users responsibility to ensure that all DLP practices are adhered to.*

3.4.2. Only files located in Google Drive are backed up. Any files on local computer drives have no backup. The IT department is not responsible for any lost data due to storage of files on locations not backed up. As an example, your desktop, downloads folder and my documents folder is NOT backed up.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that files they wish to be backed up are stored on Google Drive.*

3.4.3. The IT department will provide a 3 times daily backup to the drive environment with the ability for users to restore these backups at their discretion.

EMPLOYEE RESPONSIBILITY: *Employees are encouraged to self-serve recoveries of drive files. Information on this system can be found on the help desk site.*

3.5. Calendar

3.5.1. The IT department will provide access to a calendar system to employees whose job function requires this access.

3.5.2. Calendars can be created and shared by employees as needed, on demand.

EMPLOYEE RESPONSIBILITY: *It is the users responsibility to ensure that each calendar is shared only with other users that need access and to ensure that each calendars visibility settings are set to an appropriate level.*

3.5.3. The IT department will provide a 3 times daily backup to the calendar environment with the ability for users to restore these backups at their discretion.

EMPLOYEE RESPONSIBILITY: *Employees are encouraged to self-serve recoveries of calendar information. Information on this system can be found on the help desk site.*

3.6. Copyrighted Content

3.6.1. Copyrighted data, in which the City of Quinte West does not have ownership, should at no point be stored on City infrastructure, including but not limited to file servers, Google Drive, email, etc.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that any copyrighted data is not stored on City infrastructure, cloud infrastructure or any Google or other City contracted services.*

3.6.2. Types of copyrighted data include but are not limited to:

- Motion pictures
- Music
- Books

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to become familiar and check if content is copyrighted before storing it on City infrastructure.*

4. Passwords & Security

4.1. Password Complexity

4.1.1. A password must comply to the following complexity rules:

- At least one Number (1 - 9)
- At least one Capital Letter

- At least one Lower Case Letter
- At least one special characters for example: ! @ &) > space
- Must be at least 15 characters long

In addition to meeting these requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to use passwords with the prescribed complexity.*

4.1.2. If a particular system does not accept the above with respect to any of the factors, number of characters or types of characters, the employee is instructed to get as close to the standard as possible.

4.1.3. IT best practices for complying to the above prescribed complexity rules:

Using a few unconnected words in your password is the best way to ensure a strong password. For example: (These are not to be used!)

- Pink Octopus 3rd Hat
- Regulation 3:12 Truck Blanket
- Houston’s 7th symphony

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to use best practices when selecting passwords that meet the complexity requirements.*

4.2. Password Reuse

4.2.1. As a best practice, passwords are NOT permitted to be reused.

4.2.2. Passwords are not to be reused amongst different sites. Ie. Passwords must be unique across all different sites.

4.3. Password Change Frequency

4.3.1. Your password for Active Directory (computer user) which is linked to your Google account must be changed every 3 months.

4.3.2. Passwords for less used sites do not need to be changed but must be unique amongst different sites.

4.4. Password Care and Use

4.4.1. Passwords must remain a secret.

EMPLOYEE RESPONSIBILITY: *Employees are responsible to ensure the following rules are observed:*

- *Never give out your computer/windows, or any other site passwords to anyone.*
- *Never share your passwords with any outside parties, including those claiming to be representatives of business partners with legitimate need to access a system.*
- *Never write your password down.*
- *Never save your password in any un-encrypted manner on any device.*

4.4.2. Where user accounts are not shared, access to another individual system accounts is never to be accomplished through the sharing of an individual's system password. Delegation of accounts will be provided by the IT team through a request to the help desk.

4.4.3. Password storing and sharing will be made available using a password manager. Only the approved password manager used by the City of Quinte West will be permitted for use.

EMPLOYEE RESPONSIBILITY: *Employees are responsible to request the use of this system if needed.*

4.4.4. After five failed login attempts, your computer will lock. Contact IT to regain access at extension Help (4357).

4.4.5. If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately and the IT team notified.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to inform the IT team of any suspected account compromise.*

4.5. Building Access Cards and Devices

4.5.1. The IT team, or approved delegates, will provide a security badge with photo identification for each employee. This card will provide access to buildings and facilities that are required for the completion of City business by that employee.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to ensure they have their security badge on their person at ALL times that they are on City property or conducting City business.*

4.5.2. The photo taken for the employee ID card will be standardized for all employees. New photos can be requested as needed.

4.5.3. The IT team will provide a method through which to report lost or stolen cards.

EMPLOYEE RESPONSIBILITY: *It is the employees responsibility to IMMEDIATELY report any lost or stolen cards to IT through the use of the IT help desk. If a lost card is not reported, it could be used by someone else to access city resources.*

4.5.4. When access is required to a new location, IT will require permission from the manager or director of the appropriate department.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to request additional building access through the appropriate approving party. (Usually the manager or director of the facility to be accessed)*

4.5.5. Proper use of building security cards must be followed.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to:*

- *Ensure their card is visible at all times.*

- *Ensure no one tailgates into a secure location by observing the closure of the secured door behind them.*

4.5.6. An employee may request a guest or contractor pass for work being completed by third parties at City facilities.

4.5.7. The IT team will provide a method through which requested access is revoked to certain areas.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to inform IT if access to an employee only area is no longer required. This should be done through the IT help desk.*

4.6. Device Locking

4.6.1. The IT team will provide devices with the ability to be locked to prevent unauthorized users from accessing the device.

EMPLOYEE RESPONSIBILITY: *It is the employee's responsibility to ensure that each device they use with locking capability is configured with some type of locking method.*

4.6.2. Sharing of lock codes with any other users is strictly prohibited.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employe to not share lock codes, passwords, pins, etc… with ANY other users.*

4.6.3. Locking methods approved for use:

- Biometric (fingerprint, face)
- PIN Code
- Password

4.6.4. IT will provide a default locking mechanism when devices are delivered to employees.

EMPLOYEE RESPONSIBILITY: *The default (IT provided) lock code or method MUST be changed upon taking delivery of the device.*

4.6.5. Any device that is capable of locking automatically should be enabled to do so.

4.6.6. Phones are not to be set to stay unlocked for longer than <u>1 minute</u> of inactivity.

4.6.7. Computers are not to be set to stay unlocked for longer than <u>10 minutes</u> of inactivity.

4.6.8. IT will provide a method of locking devices when they are not in use.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that the following statement is always enforced: ALL devices MUST be locked when stepping away from the computer or device. It is also recommended that employees lock any devices that they see unlocked and unattended.*

4.7. Portable Media

4.7.1. Is enabled for use on City infrastructure and can be obtained if needed for work related purposes.

4.7.2. Portable media can be scanned upon request by the IT team in an unconnected, safe environment that does not pose a security threat to City infrastructure.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that ALL NEW portable media has been properly scanned before connecting to any City device or infrastructure. This includes, but is not limited to, USB thumb drives and memory cards that have been given to you, USB thumb drives and memory cards that have been found, etc. This can be accomplished by contacting the IT team to perform this scan.*

4.7.3. Portable media should be routinely wiped of data when not in use. After the media has completed its function, data should be removed from the device and the device formatted. This is a good practice for DLP (Data Loss Prevention).

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that DLP practices are performed to limit the loss of data due to portable media use and misuse.*

4.8. Anti-Virus

Malicious software can be transmitted via email, file attachments, downloaded content and removable media. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to the City in terms of data loss, loss of staff productivity, and/or loss of reputation.

The policies here apply to all devices on any network. This includes personally owned computers brought in by employees, contractors or consultants that may be connected to City guest networks or contractor networks.

4.8.1. All computers attached to the City of Quinte West's managed corporate networks will have Anti-Virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. This software will be installed by the IT team at the time of initial deployment.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to report any suspicious behaviour of their computer to the IT department. Especially with respect to anything involving their Anti-Virus software.*

4.8.2. Opening suspicious emails or documents is prohibited.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to never open any files, emails, macros, etc. that they suspect are malicious or are from unknown, suspicious or untrustworthy and unsolicited sources.*

4.8.3. Contractor or consultant computers should to the best of our ability comply to anti-virus policies.

4.8.4. Computers or other devices found to have been compromised will be removed from City networks until the compromise has been remediated.

4.8.5. Any activities with the intention to create and/or distribute malicious programs onto the City's systems (eg. viruses, worms, trojans, ransomware, phishing, denial of service etc) are strictly prohibited.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to :*

- *Never open any files or macros attached to an email from a known source (even another employee) if you were not expecting a specific attachment from that source.*
- *Be suspicious of email messages containing links to unknown websites.*
- *Never open any files that are executable in nature.*
- *Never copy, download or install files from unknown, suspicious, or untrustworthy sources or removable media.*
- *Avoid using portable drives. (Use our cloud services instead)*

4.8.6. Any suspicious files or email should be reported to IT immediately.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to report what they believe to be a virus or any other malicious files or emails to the IT department. Also, if the employee suspects that a computer is infected they should report this immediately.*

4.9. Phishing

4.9.1. Many data breach incidents are not caused by the compromise of City infrastructure or systems, but instead, by the compromise of humans using these systems. This type of attack is called “phishing”.

EMPLOYEE RESPONSIBILITY: *Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.*

4.9.2. Mail / Fax fraud is another form of phishing that needs to be recognized.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to use precaution when receiving unsolicited communication via mail or fax asking to perform security sensitive actions. Examples include modifying EFT information.*

4.9.3. The IT department will occasionally perform campaigns that simulate phishing attempts in order to educate employees on potential ways they could be targeted. In the event that an employee fails the test they will be contacted and given mandatory training on the subject.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee, on the failure of any phishing test campaign, to complete extra training.*

5. Guest WiFi & Third Party Access

5.1. Guest WiFi

5.1.1. Employees can sponsor both their own personal devices along with contractors and guests access to the City of Quinte West guest WiFi system.

5.1.2. Access can be granted at https://guestwifi.quintewest.io

5.1.3. When sponsoring a guest WiFi user the employee is solely responsible for the actions of that user on City networks.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to ensure that contractors and guests who access the City of Quinte West guest WiFi network adhere to the applicable sections of this policy.*

5.2. Third Party Access

5.2.1. Third party access to City of Quinte West technology, systems and property is provided on an as needed basis to authorized contractors and consultants.

5.2.2. Requests to provide access to third parties should be requested through the IT team to ensure correct levels of security and access are given.

5.2.3. At no time should an employee circumvent any system or process to give a contractor access (either physically or digitally) to any City of Quinte West system or property.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to not permit any unauthorized individuals (both employees or not) from using City of Quinte West technology, systems or services both on City property and off.*

5.2.4. Third party access will be regularly reviewed and revoked if no applicable use for the continuation of access is established. The IT team will err on the side of revoking access if any ambiguity exists.

6. Video Surveillance

6.1. Expectation of Privacy

6.1.1. The City of Quinte West does not place CCTV cameras where employees or residents can reasonably expect privacy.

6.2. CCTV use at City facilities

6.2.1. Video surveillance, when utilized with other security measures, is an effective means of ensuring the security and safety of City facilities, the individuals who use them, and the assets housed within them.

6.2.2. The City of Quinte West will follow the applicable privacy sections of the Ontario Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and will use the Information and Privacy Commissioner's guidelines in its practices related to the collection, use, sharing, storage and disposal of any information received from CCTV systems or any other system.

6.2.3. The City of Quinte West chooses locations to place CCTV cameras based on a combination of risk mitigation factors and employee safety factors.

6.3. Access to CCTV recordings

6.3.1. Access to CCTV recordings can be made through a director or HR representative.

7. Telephony Best Practices

7.1. Voicemail

7.1.1. If an employee has a City of Quinte West extension, voicemail should always be set so that callers know who they are leaving a message for.

7.1.2. The City of Quinte West phone system has the ability to email voicemails to users.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to request voicemail to be sent to email.*

7.1.3. If an employee has a City of Quinte West mobile phone, voicemail should always be set so that callers know who they are leaving a message to.

7.2. Best Practices & Accessories

7.2.1. Headsets will be provided when requested by the manager for employees whom require them to do their job.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to request a headset if needed through their manager.*

8. SaaS (Software as a Service) & Cloud Computing

8.1. General Guidelines

8.1.1. The City of Quinte West is committed to enabling the efficient use of technology and services in the completion of City business for the betterment of the residents of the City of Quinte West. To that end the following guidelines are intended to establish a process whereby the City of Quinte West employees can use cloud services without jeopardizing company data and computing resources.

8.1.2. Cloud services are NOT to be used without the knowledge of the IT department.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to NOT open cloud service accounts or enter into cloud service contracts for the storage, manipulation or exchange of City-related communications or City-owned data without the IT department's input.*

8.1.3. Use of cloud computing services for work purposes must be formally authorized by the IT department. The IT department will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

8.1.4. If you are not sure whether a service is cloud-based or not, please contact the IT department.

EMPLOYEE RESPONSIBILITY: *It is the responsibility of the employee to check with the IT department if they are unsure if the service they are evaluating is a cloud-based software system and to have it approved for use.*

8.1.5. For any cloud services that require users to agree to the terms of service, such agreements must be reviewed and approved by the IT department.

8.1.6. The use of such services must comply with all other sections of this policy.

8.1.7. Employees must not share log-in credentials with coworkers. The IT department will keep account information for business continuity purposes in a secure and encrypted manner.

8.2. Personal Cloud Services

8.2.1. Personal cloud service accounts may not be used for the storage, manipulation or exchange of City of Quinte West communication or City of Quinte West data and information.

Appendix A: Revision History

A.1 The City of Quinte West may amend this policy at any time as the City considers necessary. Affected employees will be provided notice of the changes, and shall be required to comply therewith immediately.

Date	Reference Section	Change
2019-11-01	ALL	New document. IT-2019-01 replaces all existing known or unknown IT policies.
2019-11-28	ALL	Various grammar and language changes as per Senior management review.
2019-12-10	ALL	Formatting, headers and footers.