CITY OF LANGLEY	Title: Information Technology Policy	Number: AD-09
	Authority: Senior Management Team	Section: Corporate Services
	Date Approved: November 9, 2022	
	Historical Changes ( )	

Purpose:

The intent of this policy is to protect the City, its employees, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

The purpose of this policy is to establish guidelines, security awareness and define acceptable use of information technology and electronic communications at the City. Inappropriate use exposes the City and users to risks, including cyber attacks, compromise of network systems and services, and potential legal issues.

Effective security is a team effort involving the participation and support of every City employee and user who deals with information technology and electronic communications. It is the responsibility of every system user to know these guidelines and to conduct their activities accordingly.

Scope:

This policy shall apply to all City elected or appointed officials, employees, consultants, temporary employees, and all other workers at the City, including all personnel affiliated with third parties and other non-employees utilizing electronic communications for the City. This policy applies to all equipment owned or leased by the City and any third-party devices connecting to City networks.

Definitions:

City City of Langley

Cloud services The delivery of computing services including, servers, storage, networking and software over the internet.

Electronic communication Includes but not limited to any communication or electronic file that is created, sent, forwarded, replied to, transmitted, recorded, broadcast, distributed, stored, held, copied, blind-copied, downloaded, displayed, viewed, read, faxed, electronically mailed, emailed or printed by one or several electronic communication devices or electronic communication services.

Electronic communication devices Any combination of telephones, cell phones, hand-held units, radios, telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers, laptops, tablets, mobile and notebook computers, data

processing or storage systems, computer systems, servers, data networking equipment, wireless access devices, password managing devices, input/output and connecting devices, video conferencing devices, applications, tools and related computer records, programs, software and documentation that supports electronic communication services.

***Electronic communication* record** Is a record created either intentionally or unintentionally through use of electronic communication device.

Electronic communication services Any messaging, collaboration, publishing, conferencing, broadcast or distribution system or network, including the Internet and cloud storage that depends on electronic communication devices to create, send, forward, reply to, transmit, record, store, hold, copy, download, display, view, browse, conference, read, fax, email or print electronic records for purposes of communication across electronic communication devices.

Encrypted Information that is concealed and protected in such a way that only authorized parties can read it.

Extranet An intranet that is partially accessible to authorized persons outside of a company or organization.

Internet An electronic communications network that connects computer networks and organizational computer facilities around the world.

Intranet A computer network with restricted access, as within a company, that uses software and protocols developed for the Internet.

Multi factor authentication An authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

PCI compliance The Payment Card Industry requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment.

Pirated To use or reproduce without authorization or legal right.

Port scanning The use of a software application designed to probe a server or host for open ports.

SPAM Unauthorized and/or unsolicited electronic mass mailings.

User interface The space where interactions between humans and machines occur.

VPN Virtual private network is an arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.

Policy:

General Use and Ownership

1) City issued information technology equipment, devices, and electronic communications are the property of the City and are provided for business purposes to enhance productivity and improve customer service. As with any other business tool, the City requires that information

technology equipment and electronic communications be used in a responsible, ethical and lawful manner.

2) Electronic communications shall involve City business activities or contain information related to the accomplishment of City business.

3) When communicating, users shall identify themselves honestly, accurately, and completely when sending or responding to electronic communications.

4) While the City endeavours to provide a reasonable level of privacy, users should be aware that the data (records, information) they create and store on corporate systems is subject to the Freedom of Information and Protection of Privacy Act (the Act) and, accordingly, the City has the right to request access to data contained on any corporate system used by a user in order to meet the requirements of the Act.

5) Any activity on a City-issued electronic communication device can inadvertently result in creation and/or storage of personal information on City information technology infrastructure. Accordingly, users should limit use of corporate systems for personal use in order to minimize the amount of private personal information collected by the City. For example, downloading personal documents from the internet may create records that can be inadvertently accessed by other system users if they are not properly secured.

6) Information technology users are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use should not interfere with City business and processes, and should not incur any financial charges.

7) Users must comply with all applicable laws and regulations and respect the legal protection provided by copyright and licenses for both programs and data.

8) Any information that is sensitive or vulnerable shall be encrypted and/or password protected before sending or forwarding it to a third party or external organization. If you need any assistance, please contact the IT division.

9) For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems, and network traffic at any time. This includes activities such as virus and malware monitoring, PCI compliance, suspicious network traffic, intrusion prevention, and detection.

10) The City reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Security and Proprietary Information

1) Confidential information should not be available on Internet / Intranet / Extranet-related systems. Examples of confidential information include but are not limited to: closed or in-camera council documents, credit card information, banking information, personal or customer information, customer lists. Employees should take all necessary steps to prevent unauthorized access to this information.

2) City-authorized users must keep passwords secure and must not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user-level passwords should be changed every 90 days or as set by the policy. Multi factor authentication must be used where required and while accessing systems and the City network externally.

3) All computers, laptops, and workstations should be secured with a password with the screen lock feature set at 15 minutes or less. Exceptions are added on a case-by-case basis by the City's Manager of Information Services after ensuring adequate security measures are in place.

4) City-authorized users should secure their computers by logging off or locking their devices when they are unattended.

5) Information contained on portable devices is especially vulnerable to loss or theft. City authorized users should exercise special care when removing laptops, tablets, smartphones, and other mobile storage devices from City facilities and must have security enabled to protect the device from unauthorized use.

6) Posting by employees from a City email address to newsgroups, social media, etc., should not contain personal opinions. Policy guidelines for social media remain consistent with those guidelines for traditional media. Whereas social media opens the accessibility of the medium to all staff, which may not occur in a conventional media setting, additional guidelines apply:

   - Official postings and responses representing the City must be coordinated through the City's Administration and Communication teams.
   - City information posted to these sites and services must follow all existing City policies for information.
   - When staff encounter topics on social media sites that may require a reply from the organization, communication teams should be notified to coordinate a response.

7) All devices used by City authorized users that are connected to the City Internet / Intranet / Extranet shall be running current malware and endpoint protection software if available.

8) City-authorized users must use extreme caution when opening email attachments or clicking on links. These emails may pose a cyber threat to the City.

Prohibited and Unacceptable Use

Activities that disrupt or threaten to disrupt the efficient operation of City business or administration are prohibited. City authorized users may be exempted from these restrictions during their legitimate job responsibilities (e.g., IT staff may need to disable the network access of a device if that device is disrupting services).

Under no circumstances is a City authorized user permitted to engage in any activity that is illegal under local, provincial, federal or international law while utilizing City owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of prohibited and unacceptable use.

A. System and Network Activities

The following activities are strictly prohibited, with no exceptions

1) Violations of the rights of any person or company protected by licensing, copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

2) The Manager of Information Services must be consulted before purchasing or installing any new software.

3) Accessing Office 365 and other cloud services from an unsecured personal device that could compromise network security.

4) Sensitive information and/or confidential emails should not be forwarded to personal emails, stored on personal devices or accounts hosted by third-party service providers.

5) Users shall not use internet access on a City issued device to view, download, save, receive, or send material related to or including:

   - Offensive content of any kind, including pornographic material
   - Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability
   - Threatening, violent, or illegal content
   - Gambling, dating, games, gun, or explosives

6) Introduction of malicious programs into the network or server (e.g., viruses, malware or ransomware, etc.).

7) Revealing your account password to City staff and others or allowing the use of your account by City staff and other third-party contractors or consultants. This includes family and other household members when working from home.

8) Making fraudulent offers of products, items, or services originating from any account.

9) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.

10) Port Scanning, network security scanning or any form of network monitoring unless expressly authorized by the Manager of Information Services.

11) Circumventing user authentication or security of any computer, network, or account.

12) Interfering with or denying service to any system or network user (for example, denial of service attack).

13) Providing information about, or lists of, City employees to parties outside the City. The appropriate management should be consulted prior to the export or copying of any material that is in question.

B. Email and Electronic Communication Activities

1) Electronic communication that disrupts or threatens to disrupt the efficient operation of City business and/or administration are prohibited. Electronic communications prohibited in this section include but are not limited to:

   - Electronic communications that publicize a personal dispute other than according to an approved grievance or complaint procedure.
   - Electronic communications that constitute or counsel insubordination.
   - Electronic communications that may harm close working relationships.
   - Electronic communications that are not related to City business that may disrupt or take users away from their regular duties and responsibilities.

- Electronic communications that harm the integrity of the electronic communication devices and services.
- No person shall access or utilize another person's electronic communication devices and services unless given permission to do so.
- Unless authorized, make a statement using electronic communications that implies a position or binds the City.

2) Electronic communications that violate laws, violate individual rights, or create potential liability for the City are prohibited. These prohibited electronic communications include but are not limited to:
   - Electronic communications which are pornographic, obscene or offensive.
   - Electronic communications in conflict with the City's Sexual Harassment Policy or any other policy prohibiting discrimination including harassment on the basis of race, colour, religion, sex, national origin, ancestry, age, physical disability, mental disability, medical condition, veteran status, marital status, sexual orientation or any other status protected by local, provincial or federal laws.
   - The use of racial, religious, or ethnic slurs.
   - Electronic communication intended to harass or annoy.
   - Threats that implicate a violation of personal safety.
3) Electronic communications shall not be used to solicit or recruit others for non-job-related commercial ventures, religious or political causes, outside organizations, or other non-job related activities, with the exception of City sponsored or supported services or events.
4) Electronic communications shall not be used for the sale or promotion of non-City ventures, goods, services, or events, with the exception of City sponsored or supported services or events.
5) Electronic communication devices and services shall not be used to access personal messaging services or personal email accounts or any other Internet-based electronic communication and services unless otherwise approved by the City's Manager of Information Services.
6) Electronic communication devices and services shall not be used to participate in newsgroups, chat rooms or other discussion forums unless they are specifically for City business or are specifically authorized to do so by the City's Manager of Information Services. When doing so, you shall always identify yourself and act both in the best interests of the City and in compliance with all applicable laws.
7) Electronic communication devices and services shall not be used to receive Internet-based radio or non-work-related video broadcasts and streaming services without the permission of the City's Manager of Information Services.
8) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email SPAM).

C. Management of Electronic Communication Records

1) Electronic communication records may be subject to review by City management and disclosure to the public in accordance with the Freedom of Information and Protection of Privacy Act.
2) Electronic communication records may be subpoenaed or requested under the Freedom of Information and Protection of Privacy Act and / or may be used as evidence in court or as part of an investigation.
3) As the City is responsible to protect and retain corporate electronic communication records in its custody and control, City management has the authority to access City business-related electronic communication records at any time for any City business-related reason.
4) Electronic communication records which are intended to be retained in the ordinary course of the City's business are recognized as official records that need protection and retention in accordance with the City's retention policy and schedule.
5) The City will maintain backups of all electronic communications determined to be official records as designated by the City's backup and retention schedule.

D. Electronic Communication Devices and Services

1) You shall not install or operate any new electronic communication devices on the City network without the permission of the City's Manager of Information Services.
2) You shall not access City's electronic communication services without the permission of the City's Manager of Information Services. This includes VPN and remote access using non-City supplied electronic communication devices. Users with electronic mail accounts with the City are authorized to access their electronic mail using the City's system or the Office 365 portal from a secure and authenticated device using multi factor authentication.
3) Installing unauthorized wireless access equipment to the City's network is strictly forbidden.
4) You are responsible to ensure that nobody else uses your electronic communication accounts. Passwords should therefore be kept strictly confidential. You may be responsible for any actions performed by someone using your electronic communication accounts if you provide access or share your password. You shall also never use another user's electronic communication accounts.
5) You shall not attempt to circumvent any security measures used in conjunction with electronic communication devices and services.
6) You shall not use electronic communication devices and services to deliberately propagate any virus, malware, and ransomware or to achieve unauthorized access to any electronic communication devices, services or other confidential and proprietary material.
7) When you use electronic communication devices and services, certain information identifying both yourself and the City can be recorded without your knowledge. You should therefore act on the basis that the City's name and reputation will be associated with every action taken when accessing electronic communication devices and services.
8) Electronic communication devices and services shall not be used knowingly to violate the laws and regulations of Canada or any other nation, or the laws and regulations of any state, City, province, or other local jurisdiction in any way.

9) External users, third-party contractors, and consultants are prohibited from connecting any non-city owned electronic devices to a network port or secured network connection in City facilities. The City representative must ensure that the City's network and perimeter security is maintained by informing external users about these requirements. Wi-Fi Services are provided in City facilities to meet internet connection requirements.

E. Cloud Services

1) You shall not install or subscribe to cloud service initiatives for the City without the permission of the City's Manager of Information Services.
2) You shall not attempt to circumvent any security measures used in conjunction with cloud services offered by the City.

F. Malicious Software and Spam

1) Software should not be downloaded or installed on City issued devices and/or City networks without the permission of the City's Manager of Information Services. Even seemingly harmless programs, such as Internet search bars and weather update services, can install malicious software, including viruses, malware and ransomware without your knowledge.
2) Do not install software or files from home or electronic media such as CDs, DVDs, or external USB drives. Do not plug in USB drives or portable media from the public, third-party contractors, or consultants to a City-issued device without the permission of the City's Manager of Information Services. Upon approval, a malware scan must be completed on all external portable media devices.
3) The City has protection against malicious software on its electronic communication devices and services. It is recommended that users install a complete suite of protective software on their personal electronic communication devices if used for accessing City's webmail, office 365 services, and other cloud services. It is also recommended that protective software be installed and kept up-to-date on any non-City owned electronic communication devices and services used by staff or third-party contractors to conduct City business such as consulting, training or presentation in a City facility.
4) Users must immediately report suspicious electronic communication activities or the detection of viruses or other harmful files to the City's Manager of Information Services.
5) Do not respond to unsolicited commercial electronic mail ("spam") or click on "unsubscribe from the list" or any other links. Users are required to report spam using any of the reporting tools to City's IT staff or permanently delete all spam electronic communications.

G. Unauthorized Monitoring of Electronic Communications

1) It is a violation of City policy for any user, including systems administrators, supervisors, or programmers to use electronic communication devices and services for satisfying idle curiosity about the affairs of others, for obtaining access to electronic communications of others with no substantial business purpose or legal authority. Abuse of authority by accessing electronic communications for such purposes is prohibited.

Enforcement

Any employees, elected or appointed officials, contractors, consultants, temporary employees, and all other workers at the City, including all personnel affiliated with third parties found to have violated this policy, may be subject to disciplinary action.

All users will be provided a copy of this regulation upon granting access to the City's electronic communication devices and services. Each user shall be required to complete an acknowledgment in substantially the form attached hereto as Attachment "A" and Attachment "B" which will be maintained by the Manager of Human Resources.

1) Failure on the part of any employee to comply with the provisions of this policy shall subject the user to disciplinary action up to and including dismissal. Further, failure to comply with any provision of this policy may result in suspension or revocation of the privilege of using or accessing electronic communication devices and services.
2) Failure on the part of any City elected or appointed official to comply with the provisions of this policy will constitute grounds for the City Council to suspend or deny official access to electronic communication devices and services and may be subject to the provisions under other bylaws and policies pertaining to Council members.
3) Failure on the part of any contractor, consultant, or other non-employees utilizing electronic communications to comply with the provisions of this policy will constitute grounds for termination of their contract with the City.

References:

Policy Number:	**AD-09**
Policy Owner:	**Corporate Services**
Endorsed by:	**Senior Management Team**
Final Approval by:	**Senior Management Team**
Date Approved:	**November 9, 2022**
Revision Date:	
Amendments:	
Related Policies:	
Related Publications:	

Contact Person:

Contact Person: Mathew Jose
Position: Manager of Information Services
Phone: 604-514-2811
Email: mjose@langleycity.ca

ATTACHMENT "A"

CITY OF LANGLEY USER ACKNOWLEDGEMENT OF INFORMATION TECHNOLOGY POLICY

I hereby acknowledge that I have read and understood the City's Information Technology Policy in its entirety and will comply with requirements as set therein.

I understand that the City's electronic communication devices and services are for City business use only and while the City endeavours to provide a reasonable level of privacy, users should be aware that the data (records, information) they create and store on corporate systems is subject to the Freedom of Information and Protection of Privacy Act (the Act) and, accordingly, the City has the right to request access to data contained on any corporate system used by a user in order to meet the requirements of the Act. The City has the right to request access to city devices at any time to review compliance with this Policy. Finally, I understand that violation of this Policy may result in disciplinary action or termination of contract.

I acknowledge that upon the end of my employment, ceasing holding an elected office or end of contract with the City of Langley, I will return the City issued device(s) to the City for examination and removal of City records and data. Upon completion, City provided devices will follow established reclamation or disposal procedures.

Name: _____

Signature: _____

Date: _____

ATTACHMENT "B"

CITY OF LANGLEY USER ACKNOWLEDGEMENT OF MICROSOFT 365 SERVICES, DATA COLLECTION AND DEVICE MANAGEMENT POLICY

The City of Langley provides select staff and members of the Council with mobile phones, data devices, laptops, and tablet devices for work purposes that will have access to corporate email and files. Other staff may elect to leverage personal devices for work purposes. These devices will be managed by a cloud service hosted by Microsoft Corporation, a multinational technology company with headquarters in Redmond, Washington, United States, that provides services for the security needs of corporate data and includes functionality required to secure that corporate data.

The data collected is essential to centralized device management and is required to provide the functionality offered by the solution. Data is collected from end-user devices that are managed by the solution as well as third-party solutions that may be integrated with the solution.

Data collected and stored by this service includes:

- User information
    - Owner name/User Display Name
    - User Principal Name (Email Address)
    - Third-party User Identities (i.e., AppleID)
- Hardware inventory information
    - Device Name
    - Device Manufacturer
    - Operating System
    - Serial Number
    - IMEI Number
    - IP Address
    - Wi-Fi Mac Address
    - ICCID
    - Phone Number
- Access control information
    - Static authenticators
    - Privacy keys for certificates
- Application inventory, including:
    - Application Name
    - Application Version
    - Application ID
    - Size
    - Installation Location
- Customer 3rd party tenant IDs, like the Apple ID
- Usage/Census/Error Reporting Data

Data associated with this service is stored at rest in the United States of America and is encrypted for security purposes. Access to that data is limited to City staff and Microsoft technical support personnel who are guided by terms of service restricting access to that data. It is not accessible to third parties and will not be shared by Microsoft with third parties.

Any personal information collected by the City of Langley in connection with Microsoft programs will be collected for Office Productivity and Collaboration purposes under the authority of s.26(c) of the Freedom of Information and Protection of Privacy Act (FOIPPA). Personal information may also be accessed, exchanged, or collected to facilitate interactions between staff for the purposes of Office Productivity and Collaboration under the authority of s.27 of FOIPPA. If you have any questions about this collection, please contact:

Kelly Kenney, Corporate Officer
604.514.4591

20399 Douglas Crescent
Langley, BC V3A 4B3

Consent:
I understand that information may be collected from my corporate device and may be used and disclosed for the purposes outlined above. This consent will be considered valid from the date at which it is signed until I no longer require the use of City-supplied devices and software. I acknowledge that upon my end of employment or term with the City of Langley, I will return the City issued device(s) to the City for examination and removal of City records and data.

I also hereby acknowledge that I have read this consent form and understand that information will be collected from my device and may stored outside of Canada.

Name: _____

Signature: _____

Date: _____

This form must be signed, dated, and returned to Corporate Services before a corporate device may be issued to a user of the City of Langley. If a user has already been enrolled in receiving these services with a device such as a phone, tablet, or laptop with data access, it must be returned if consent is not provided.

Legislation that governs the use of confidential and personal information

1. ***The Freedom of Information and Protection of Privacy Act (FoIPPA):*** FoIPPA is mandatory legislation that governs all aspects of managing personal information, including its collection, use, and disclosure.
2. ***Freedom of Information and Protection of Privacy Regulation:*** The FoIPPA Regulation supports the application of FoIPPA with regard to purposes for collecting personal information, disclosure of personal information, and consent to collect personal information on someone else's behalf.
3. ***Personal Information Protection Act:*** PIPA is the privacy legislation that most privacy companies, organizations etc., must comply with to manage personal information.
4. ***The Personal Information Protection and Electronic Documents Act (PIPEDA):*** This is federal privacy legislation that federally regulated companies must comply with to manage their personal information.