TOWN OF
Tecumseh
ONTARIO · CANADA

The Corporation of the Town of Tecumseh

Policy Manual

Policy Number:	**09**
Effective Date:	Click here to enter a date.
Supersedes:	**June 25, 2013**
Approval:	
Subject:	**Technology Acceptable Use Policy**

Table of Contents

1.0 Purpose

1.1 The purpose of this policy is to establish specific requirements to support efficient, cost-effective and secure use of major information technology (IT) infrastructure and resources.

1.2 In general, acceptable use shall be taken to mean respecting the rights of other digital users, the integrity of physical and digital assets, pertinent license and contractual agreements, and where applicable, maintaining compliance with legal and regulatory requirements.

1.3 This policy will be used to protect the Town of Tecumseh ('Town') in relation to technology and telephony use, against hazards such as:

1.3.1 Unauthorized access and intrusion

1.3.2 Malicious manipulation and/or destruction of information/data

1.3.3 Virus or spyware invasion

1.3.4 Inappropriate use

1.3.5 Litigation due to misappropriation of software and/or data OR misuse of equipment

1.3.6 Inappropriate disclosure of confidential information

1.4 The policy will outline the underlying principles and rules that govern the use of the Town's IT resources including acceptable use of internet, electronic messaging, networks, computers, applications, data access and mobile devices.

2.0 Scope

2.1 This policy applies to all Town staff, elected officials, volunteers, consultants and contractors. It does not apply to the members of the public using publicly available Wi-Fi or internet access.

3.0 Definitions

3.1 **Authentication Token**: A physical device that an authorized user is given to ease authentication or to provide multi-factor authentication.

3.2 **Business Record**: Any recorded information, whether in printed form, on film, by electronic means or otherwise, created or received by the Town in the conduct of business, including electronic messaging applications capable of producing a record.

3.3 **Cardholder Data:** At a minimum, cardholder data consists of the full Primary Account Number (PAN), it may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

3.4 **Cloud Computing:** A cloud computing model in which data is stored on remote servers and is made available over the Internet. It is maintained, operated and managed by a cloud storage service provider.

3.5 **Computing and Telecommunications Facilities**: Any device owned by the Town that is used to access, store, process or transmit information, including but not limited to personal computers, tablets, kiosks, network, servers, applications, telephones, pagers, radios, smartphones, geographic positioning devices, or other similar devices.

3.6 **Corporate Computing Devices**: Any computing device that was procured, configured or is being managed by TCS.

3.7 **Corporate Data**: Data and information that is owned, collected, stored, processed, and shared by the Town. This can include financial data, customer data, employee data, operational data, and any other data that is necessary for the functioning of the corporation.

3.8 **Council**: the Council of the Corporation of the Town of Tecumseh

3.9 **E-mail:** (Electronic Mail) a system for sending and receiving messages electronically over a computer network, as between personal computers.

3.10 **Employee**: any person employed by the Town on a full-time, part-time, seasonal, student and/or casual basis, as well as volunteers, contract workers and Committee Members.

3.11 **Information:** Any electronically stored content, including but not limited to data, records, documents, files, logs, images, audio and video.

3.12 **Internet:** an electronic communications network that connects computer networks and organization computer facilities around the world.

3.13 **Mobile Device**: A portable computing device such as a smartphone or laptop.

3.14 **Password**: The individual personal password or security code assigned to the user's user ID, which may be updated by the user from time to time.

3.15 **Personal Use**: use of a computer, mobile phone, or network for activity that is not related to Town business.

3.16 **Public Wi-fi**: a public wireless networking technology that uses radio waves to provide wireless high-speed internet access.

3.17 **Removable Electronic Media:** Any device that can store data in electronic format and can be attached to various electronic devices, examples of removable electronic media include optical discs (Blu-ray discs, DVDs, CDs), memory cards (ex. USB memory stick), portable hard drives.

3.18 **Personal Computing Devices**: Any electronic equipment controlled by a central processing unit (CPU), including desktop and laptop computers, smartphones and tablets.

3.19 **TCS:** The Technology & Client Services Department.

3.20 **Town**: The Corporation of the Town of Tecumseh.

3.21 **User:** Any individual who uses Town computing and telecommunications facilities, including but not limited to Town elected officials, employees, volunteers, contractors, consultants and the public.

3.22 **User ID:** The individual user identification name or code assigned by TCS.

4.0 Computing and Telecommunications Facilities

4.1 Acceptable Use

4.1.1 Users shall not copy, destroy or alter any data, documentation, or other information that belongs to the Town or any other business entity without authorization.

4.1.2 Users shall not allow any unauthorized third parties to access the Town network and resources.

4.1.3 Users will take all reasonable steps to protect and keep secure physical, intellectual and information assets accessed through Town computing and telecommunications facilities.

4.1.4 The user will utilize Town computing and telecommunications facilities for the conduct of the Town’s business activities and as required by their specific job functions or compliant personal use.

4.1.5 The users must not use or install any software on their Town issued device including personal software or software for which the user has not been granted the appropriate license and approved by a department manager and/or TCS.

4.1.6 The user will not attempt to enter restricted areas of computing and telecommunications facilities or the computer system(s) of any entity related to or affiliated with the Town or perform functions which the user is not authorized to perform pursuant to this policy.

4.1.7 Upon retirement, layoff, resignation or termination of employment contract the users must promptly return (without duplicating or summarizing), any and all electronic records pertaining to the Town’s business as well as all electronic devices issued by or paid for by the Town, including but not limited to laptops, smartphones, etc.

4.1.8 Devices that require user authentication, such as PCs, laptops, smartphones, etc. must not be left in the unlocked state when unattended.

4.1.9 Users shall ensure that all their actions are in compliance with all applicable laws, regulations, policies and by-laws.

4.1.10 Users shall only allow remote connections to Town Computing and Telecommunications Facilities that are approved by TCS.

4.1.11 All Town business records, if located, created or received outside of the Corporate systems shall be transferred to the appropriate Corporate system as soon as possible after creation or receipt (please note that documents received during the course of business from external sources are also considered official Town business records).

4.1.12 The Town may not provide extracts of user’s personal data stored on any of the corporate computing and telecommunication facilities upon the termination of the employment relationship.

4.1.13 Users should avoid saving business critical data to local drives on their Town issued computer as this data will not be automatically backed up and might be lost due to hardware or software failure. File storage that includes automatic backups of shared drives found in Microsoft One Drive, the corporate Microsoft Sharepoint site and network file storage.

4.1.14 Users must not connect personal devices to any of the Town corporate networks, except for the public Wi-Fi network and those approved through the Town's Bring Your Own Device (BYOD)a policy.

4.1.15 Port scanning, security scanning, network mapping and network packet capture activities are all expressly prohibited, unless pre-authorized by TCS.

4.1.16 Cardholder data must not be stored on any Corporate file storage system.

4.1.17 TCS has a complete inventory of Town issued devices. Any changes in ownership of these devices assigned to users by TCS must be immediately reported to the IT Help Desk. When no longer required, all Town issued devices must be returned to TCS

4.2 Enforcement and Monitoring

4.2.1 TCS may monitor, audit and report on user activity to ensure compliance to corporate policies as well as in the event of an authorized audit or investigation.

4.2.2 Any content stored on the corporate infrastructure or devices found to be in violation of licensing agreements or copyright laws will be removed.

4.2.3 To enforce the this policy and to protect corporate information assets, TCS may deny network access to any device upon detection of unauthorized activity.

4.2.4 The Integrity Commissioner can, at any point and without additional authorization, request any electronic data processing records, reports, files or property belonging to or used by the Town that the Integrity Commissioner believes to be necessary for an inquiry. Information recovery would be managed as per the processes defined by the Legislative Services / Clerks department.

5.0 Digital Identity

5.1 Acceptable Use

5.1.1 In the event that a User forgets or believes that their password has become compromised, the User must inform the TCS Help Desk immediately.

5.1.2 Users must only use a user ID authorized to them by TCS.

5.1.3 Users must not share their passwords or any authentication tokens assigned to them by TCS with any other person.

5.1.4 Password length and complexity for every user is defined by TCS and must be adhered to by all users.

5.1.5 Corporate passwords must not be used for personal accounts (i.e. banking, personal email, social media) and vice versa - personal passwords should not be used for corporate accounts.

5.1.6 Passwords shall not displayed in written or printed form (example: near a workstation / desk / office).

5.2 Enforcement and Monitoring

5.2.1 TCS (or appointed third party network monitoring consultant) may suspend user’s access to Town computing and telecommunications facilities by deactivating account(s) if unauthorized or suspicious activity is detected.

6.0 Mobile Devices

6.1 Acceptable Use

6.1.1 Users of a corporate personal computing device is responsible for ensuring adequate physical security of the device.

6.1.2 Unless as approved under the Town’s BYOD Policy, corporate data must not be stored on any non-corporate mobile device.

6.1.3 Users must not subvert any corporate device’s security controls deployed by TCS via hacks, jailbreaks, software changes and/or security setting alterations.

6.1.4 Users must regularly install updates deployed by TCS, device manufacturers or software vendors.

6.1.5 Users must report lost or stolen corporate devices immediately to the TCS Help Desk.

6.1.6 Users must not host open (non-password-protected) Wi-Fi hotspots on corporate mobile devices.

6.1.7 User shall not install any smartphone applications from unauthorized sources. An up-to-date list of authorized mobile application sources will be maintained by TCS.

6.1.8 The Town will not provide extracts of user’s personal data stored on any of the corporate computing and telecommunication facilities upon the termination of the employment relationship.

6.2 Personal Use

6.2.1 Limited and reasonable personal use of corporate mobile devices is allowed and is limited to the following parameters, and shall not:

6.2.1.1 Have a negative impact on user productivity or efficiency.

6.2.1.2 Interfere with normal business operations.

6.2.1.3 Exceed reasonable time limits or duration.

6.2.1.4 Cause expense in the form of storage, financial or network overhead to the Town.

6.2.1.5 Compromise the integrity and security of the Town's resources or assets.

6.2.1.6 Violate any policies, procedures, by-laws, regulations or laws.

6.2.1.7 The Town shall be reimbursed by the user for any non-business related charges by the cellular carrier that are incurred on the mobile device.

6.3 Enforcement and Monitoring

6.3.1 All corporate mobile devices will be centrally managed and controlled by TCS via a mobile device management (MDM) system.

6.3.2 Devices found to be in violation of corporate security standards or this acceptable use policy may be remotely disabled, wiped or disconnected from various corporate services including the Town's internal network.

7.0 Removable Electronic Media and Cloud Storage

7.1 Acceptable Use

7.1.1 Users must not copy data to portable electronic media unless authorized by TCS including security measures.

7.1.2 Corporate cloud storage must only be accessed from Computing and Telecommunications Facilities that are issued by TCS.

7.1.3 Users shall not configure synchronization of corporate cloud storage to non-corporate devices.

7.1.4 Corporate information must not be shared with "public" or "everyone" using cloud storage; specific people or groups must be used.

7.1.5 Microsoft OneDrive when accessed using corporate (@tecumseh.ca) account is currently the only authorized secure cloud storage provider suitable for corporate information storage. Users shall not copy corporate data to any of the other third party cloud storage providers (e.g. Google Drive, Dropbox, Amazon Cloud Drive, etc.) without authorization from TCS.

7.1.6 Use of approved corporate cloud storage is only allowed for conducting Town business activities and as required by user’s specific job functions.

7.1.7 Users are responsible for managing permissions of their corporate cloud storage to ensure security of corporate data.

7.1.8 Users must consider sensitivity of information being placed on corporate cloud storage and, if required, protect it with encryption. An up-to-date list of corporate tools authorized for secure file encryption will be maintained by TCS.

7.1.9 Users must only use systems authorized for secure information exchange when sharing personally identifiable or sensitive information with other organizations. An up-to-date list of corporate systems authorized for secure information exchange will be maintained by TCS.

7.1.10 Users must consider all legislative and regulatory requirements, policies, guidelines and by-laws prior to placing corporate data on cloud storage.

7.2 Enforcement and Monitoring

7.2.1 TCS will restrict the use of removable electronic media on client PCs.

7.2.2 TCS may, through policy enforcement and any other technical means, limit the ability of users to transfer data to and from specific resources on the corporate network.

7.2.3 In specific situations, TCS may establish audit trails to track the attachment and utilization of external storage devices.

7.2.4 TCS may monitor, audit and report on activities and information being accessed, stored and transmitted to and from cloud storage to ensure compliance with corporate policies.

8.0 Internet

8.1 Acceptable Use

8.1.1 Users of the Town corporate internet may use the internet only to complete their job duties, under the purview of the Town business objective. Permissible, acceptable, and appropriate Internet-related work activities include:

8.1.1.1 Researching, accumulating, and disseminating any information related to the accomplishment of the users assigned responsibilities.

8.1.1.2 Collaborating and communicating with other users, business partners, and customers of the Town, according to the users assigned job duties and responsibilities.

8.1.1.3 Conducting professional development activities (e.g. news groups, chat sessions, discussion groups, posting to bulletin boards, web seminars, etc.) as they relate to meeting the users job requirements. In instances where the personal opinions of the user are expressed, a disclaimer must be included asserting that such opinions are not necessarily those of the Town.

8.1.2 Users shall not download files from the Internet unless their use is required for the purposes of conducting Town business.

8.1.3 Users shall not engage in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.

8.2 Personal Use

8.2.1 Limited and reasonable personal use of Internet access is defined as any personally conducted online activity or Internet usage for purposes other than those listed in s. 8.1 of this policy. Personal use is limited to the following parameters and shall not:

8.2.1.1 Have a negative impact on user productivity or efficiency.

8.2.1.2 Interfere with normal business operations.

8.2.1.3 Exceed reasonable time limits or duration.

8.2.1.4 Cause expense or network overhead to the Town.

8.2.1.5 Compromise the integrity and security of the Town's resources or assets.

8.2.1.6 Violate any policies, procedures, by-laws, regulations or laws.

8.3 Enforcement and Monitoring

8.3.1 TCS may monitor and log internet traffic for the purpose of enforcing acceptable use policies and may block access to certain websites for which access is deemed to be a contravention of this policy.

8.3.2 TCS will work with the user, supervisor and People & Culture in the event the parameters of section 8.2.1 are violated.

9.0 E-Mail

9.1 Acceptable Use

9.1.1 All Town business e-mail communications must be conducted through @tecumseh.ca e-mail accounts

9.1.2 Email communication with external organizations is not considered a secure method of information exchange. An updated list of corporate systems currently authorized for secure information exchange will be maintained by TCS.

9.1.3 Users e-mail communications must be conducted professionally and meet all requirements set forth in the Town's Employee Code of Conduct policy.

9.1.4 Users are responsible for managing their corporate mailbox permissions to ensure security of corporate data.

9.1.5 The Town may not provide extracts of user's personal data stored on any of the corporate computing and telecommunication facilities upon the termination of the employment relationship.

9.1.6 Prior to opening any attachments or opening links included in emails, users must inspect the email contents for following risk indicators such as:

- Poor formatting, spelling and grammar mistakes
- [External] mark in the message inbox
- Unknown sender or sender who does not typically send such emails
- Generic greetings
- Requesting personal or confidential information

- High urgency
- Lack of appropriate corporate branding in the email or in linked webpages

9.1.7 Emails exhibiting several risk indicators must be reported and submitted to the TCS Help Desk for further instruction.

9.2 Enforcement and Monitoring

9.2.1 TCS may monitor, audit and report on users e-mail activity and information being sent or received using corporate e-mail systems to ensure compliance with corporate security and privacy obligations.

9.2.2 TCS will provide Cybersecurity Awareness Training to all new users and on a regular basis for all users.

9.2.3 TCS may periodically conduct simulated email phishing campaigns as part of the security awareness training program. User responses including clicking links, downloading files, or providing credentials will be captured for overall security posture and risk evaluation purposes. Additionally, follow-up security awareness training and mitigation up to and including disciplinary action may be imposed.

10.0 Teleconferencing

10.1 Acceptable Use

10.1.1 Corporate standard teleconferencing solutions include TCS authorized platforms such as Microsoft Teams. Any other system might not include industry standard security and privacy controls or possess necessary meeting controls to prevent misuse and will not be allowed by TCS.

10.1.2 While conducting teleconferencing sessions with any corporate standard teleconferencing or other solution, users must employ appropriate risk mitigation controls, including but not limited to:

10.1.2.1 Enable password protection for meetings when appropriate;

10.1.2.2 Provide links only to specific people and avoid advertising on social media or other publicly available forums, unless absolutely necessary;

10.1.2.3 Ensure screen sharing and file sharing permissions are managed to prevent any unauthorized person(s) from access or viewing content; and, 10.1.2.4 Always use the latest version of the teleconferencing client.

11.0 Working Remotely

11.1.1 Users must not plug-in or connect any personal electronic devices, which were not explicitly authorized by TCS, to corporate PCs, laptops, smartphones, networks. This includes personal printers, hard drives, USB keys, cameras, microphones, computers, etc.

11.1.2 Users must not use Virtual Private Network (VPN) services not explicitly authorized by TCS, such as Express VPN, IPVanish, NordVPN, etc. while using any corporate IT services such as cloud storage, productivity applications, email, etc.

11.1.3 Users must ensure that any home wireless being used is password protected and that any default wireless router passwords have been changed.

11.1.4 Configuration that includes any personal devices will not be assessed or supported. Upon engaging IT Help Desk to troubleshoot any problems, users will be asked to remove any personal devices that might be affecting application or service.

11.1.5 Any printing required should be done at the employee’s designated Town facility workspace. Personal peripheral device (e.g. printer) that are connected to Town laptops will not be supported by TCS.

11.1.6 Use of public wi-fi when accessing the internet with corporate devices is discouraged. An up-to-date list of approved methods for connecting via public wi-fi will be maintained by TCS.

12.0 Sanctions and Violations

12.1.1 Any users found to have breached this policy, may be subject to disciplinary action.

12.1.2 Any violation of the policy by a temporary worker, consultant or supplier may result in the termination of the contract or assignment.

Any violation of this policy will be considered a breach of the Town’s Employee Code of Conduct or the Town’s Council Code of Conduct as applicable.

13.0 Relevant Legislation and Policies

13.1 057 – Confidentiality of Information Policy

13.2 061 – Accountability and Transparency Policy

13.3 063 – Council Code of Conduct

13.4 064 – Progressive Discipline Policy

13.5 Employee Code of Conduct

13.6 066 – Accessible Customer Service

13.7 069 – Use of Corporate Resources for Elections

13.8 076 – Corporate Communications Policy

13.9 080 – Social Media Policy

13.10 097 – Customer Service Policy

13.11 112 – Flexible Work Arrangements Policy

13.12 115 – Bring your Own Device (BYOD)

13.13 117 – Electronic Monitoring of Employees Policy

13.14 Privacy Policy

13.15 Municipal Freedom of Information and Protection of Privacy Act

13.16 Corporation’s Records Retention By-law No. 2018-39