

TOWN OF SLAVE LAKE			
INFORMATION TECHNOLOGY POLICY			
Directorate	Corporate Services		
Department:	Information Technology	Policy No:	CRS.IT-23.1002
Policy Title:	Acceptable Use of Information Technology	Issue Date:	
Issued to:	All Employees	Policy Type:	New

I. Policy Statement

The Town of Slave Lake offers elected officials, employees, volunteers, and other individuals (referred to as "Users") a range of resources, including computers, email, mobile devices, printing, fax capabilities, data networks, software, and additional technological tools (referred to as "Town Information Technology"). These resources are provided to enhance the execution of tasks related to the Town. All individuals who utilize Town Information Technology are expected to adhere to relevant federal and provincial laws, the specific guidelines set forth in this Policy, and all other applicable Town policies.

2. Purpose:

This policy aims to create a structured framework of rules that define the permissible usage boundaries of Town Information Technology within the town. Additionally, it outlines guidelines for the responsible and suitable utilization of this technology

3. Scope:

This policy is relevant to the utilization of all Town Information Technology resources owned, leased, or licensed by the Town of Slave Lake. Its scope encompasses these resources regardless of their geographical location.

Definitions

Personal Computing Device: Any privately owned computing device or its related components, including but not restricted to desktop computers, laptops, smartphones, handheld devices, tablets, mice, keyboards, monitors, storage devices, and network peripherals.

Mobile Client Computing Technology: Encompasses devices like cell phones, smartphones, laptop computers, tablet computers, and mobile internet sticks. This category also encompasses the usage plans associated with these devices and their corresponding peripherals.

Social Media:

This includes all forms of online presence or publications, spanning platforms such as YouTube, Facebook, Twitter, Instagram, blogs, wikis, and others, which provide opportunities for social networking activities or content sharing on the internet. Additionally, this definition encompasses social messaging applications like chat, SMS, MMS, and related software.

Cloud-based IT Service:

A service accessible to users via the internet, hosted on the infrastructure of a cloud computing provider rather than a company's own on-premises servers. This classification encompasses a range of services, such as online file storage (e.g., Dropbox), web-based email services (e.g., Gmail), and document collaboration services (e.g., Google Docs).

5. General Acceptable Use Guidelines

Town Information Technology is primarily provided to Users for the purpose of conducting Town-related activities. Limited personal use of Town Information

Technology is allowed in accordance with the guidelines specified in the "Acceptable Use" section below.

All information transmitted, received, or stored using Town Information Technology is considered Town information and falls under the jurisdiction of the Town. This includes documents, correspondence, emails, database records, and internet browsing history, among other things. The Freedom of Information and Protection of Privacy Act (the FOIP Act) applies to all Town information, potentially leading to its disclosure under the Act. The Town is committed to cooperating with reasonable requests from law enforcement, regulatory agencies, and FOIP requests for information that falls under the scope of the Act.

Moreover, the Town reserves the right (though not the obligation) to monitor the usage of Town Information Technology under certain circumstances and may exercise this right as needed.

Individuals seeking to engage in personal use of Town Information Technology with an expectation of privacy should opt to utilize a personal computing device instead.

Acceptable Use

- Town Information Technology is primarily provided to users for the purpose of conducting Town-related activities. This includes, but is not limited to, creating correspondence and reports, communicating via emails, participating in social media interactions, and utilizing the internet.
- Personal use of Town Mobile Devices is permitted, as long as it doesn't hinder Town operations and doesn't pose risks to the Town's assets, staff, reputation, or data.

Unacceptable Use

This policy strictly prohibits the use of Town Information Technology in the following manners:

- Accessing Town Information Technology, information, or accounts without proper authorization.
- Sharing personal IT account credentials (including user IDs and passwords) with others to allow unauthorized access, unless expressly authorized by Town IT for valid reasons.
- Accessing, generating, publishing, storing, or transmitting information containing the following content:
 - Content related to gambling.
 - Pirated, hacked, or unlicensed content.

- Pornographic or adult content.
 - Material promoting illegal activities.
- Content that could be interpreted as racist, defamatory, discriminatory, or hateful.
- Engaging in entertainment software, gaming, or online games against opponents.
- Uploading software or data owned or licensed by the Town without proper authorization from the respective software or data manager.
- Replicating or transferring Town information beyond the Town's network unless explicitly sanctioned by the Town Clerk or their delegate.
- Intentionally disrupting the normal functioning of the Town, its partners, or stakeholders using Town Information Technology.
- Using Town Information Technology for personal gain or profit.
- Engaging in defamatory, libelous, threatening, harassing, or offensive behavior, even under the pretext of 'course of business'.
- Transmitting copyrighted, confidential, or protected information to unauthorized individuals or the public.
- Unauthorized access to copyrighted, confidential, or protected information.
- Participating in activities that could be construed as a violation of the Criminal Code.
- Deliberately distributing malicious content like viruses, malware, ransomware, or any components that could compromise or damage another electronic device.
- Undermining the reputation and integrity of the Town or its employees.
- Sending unsolicited messages, including "junk mail" or other advertising content, to recipients who have not requested such material.
- Initiating any form of harassment through Town Information Technology.
- Impersonating other individuals or organizations.
- Soliciting individuals or organizations with the intent to harass or obtain unauthorized information.
- Creating or forwarding "chain letters," "Ponzi" schemes, or any type of "pyramid" schemes.

6. Software

- Approval from Town IT is required for all software installed on Town-owned Information Technology devices, except for cases outlined in Policy CSR.IT-23.1001 Mobile Client Computing Technology. Any software installed on Town Information Technology must comply with the licensing agreements specified by the software supplier.

7. Internet Use

Internet use must align with the regulations set forth in Section 5: General Acceptable Use Guidelines for Town Information Technology.

The Town maintains records of internet activities, and legal obligations under the Freedom of Information and Protection of Privacy Act might necessitate disclosing these records to the public.

8. Email & Communications

The use of email and other communication methods involving Town Information Technology must adhere to the guidelines outlined in Section 5: General Acceptable Use Guidelines.

As previously mentioned, the Town keeps records of both internet and email activities, and legal requirements may mandate sharing these records with the public.

9. Personal Use of Social Media

Limited and occasional use of Town Information Technology for personal engagement on social media platforms is permissible, provided it is conducted professionally and responsibly. This use should not violate this policy or other Town policies, disrupt an employee's regular work responsibilities, and adhere to the following restrictions:

- Sharing Town information on social media or internet platforms that is confidential or not approved for public release is prohibited.
- Users cannot present comments, opinions, or statements on social media or internet platforms as reflective of the Town's stance without prior approval.
- Posting comments, opinions, or statements on social media or internet platforms that could damage the Town's reputation or go against its core values is not allowed.
- Engaging in any social media activity that could harm the Town's reputation, its employees' goodwill, or the trust of its constituents is not permitted.
- While using social media, users must refrain from attributing personal statements, opinions, or beliefs to the Town. If users express personal views on blogs, they must not overtly or implicitly present themselves as Town employees or representatives.

Users acknowledge and assume all risks associated with their personal use of social media.

10. Personal Computing Devices

External Storage Devices:

External storage devices like memory sticks, CDs, DVDs, and removable hard drives may be used only when network connectivity is unavailable or when secure data transfer alternatives are not available.

Other Computer Peripherals:

Staff members should not connect any personal computing device or peripheral to Town Information Technology without explicit approval from the IT department. This includes but is not limited to monitors, mice, keyboards, laptops, network devices, and printers. Personal smartphones are allowed to connect to the Town's guest Wi-Fi network.

11. Mobile Communications Devices

This policy fully applies, as relevant, to all Town Mobile Devices provided to Town staff. Additionally, Policy CSR.IT-23.1001 Mobile Client Computing Technology outlines the specific terms governing the issuance and use of all Town Mobile Devices by Town staff.

12. Cloud-Based IT Services

Use of externally hosted IT services for storing or sharing Town information is prohibited unless explicitly authorized by IT and compliant with FOIPPA regulations. This prohibition encompasses the storage or sharing of Town-owned information, particularly personal or confidential data, through services not owned, managed, or controlled by the Town. Examples of such services include social networking applications (including all social media, blogs, and wikis), file storage and sharing services (e.g., Dropbox), external email services (e.g., Gmail), content hosting services, as well as cloud synchronization and backup services for mobile devices (e.g., iCloud, Evernote, OneNote).

Any exceptional cases must be routed through both the Town Clerk's Office and the IT Department. Users seeking clarity on what qualifies as confidential information should consult the Town Clerk's Office.

13. Policy Violations


Any violation of this policy may result in disciplinary measures, including the suspension of user privileges, removal from the system, termination, initiation of legal charges, and/or other lawful actions.

14. Exceptions

The Chief Administrative Officer holds the authority to grant standing or one-time exemptions to this policy in cases where valid business reasons exist.

15. Other Related Policies

- CSR.IT-23.1001 – Mobile Client Computing Technology
- CSR.IT-XX.XXXX - Town Client Technology Standards

ISSUED BY	APPROVED BY:	DATE:
1. Chief Administrative Officer		Sept. 15/23

