

Title: Acceptable Use of Technology Resources**Resolution: 2024-0333 Dec 9/24****Revised:****Next Review Date: 2029****Special Notes/ Cross Reference:****Policy Statement:**

The Town of Westlock is committed to safe and responsible use of technology resources to protect the Town's reputation and ensure responsible use of taxpayer dollars.

This Policy protects the interests of both the Town and the users of the Town's technology resources by providing a standard by which questions of acceptable technology resource use may be gauged.

Purpose:

The purpose of this administrative policy (policy) is to describe what the Town expects regarding acceptable, ethical and safe uses and monitoring of Town technology resources.

Scope

1. This policy applies to all Technology Resource Users (Users).
2. Users are deemed to have given consent to this policy by their continued use of the Town's Technology Resources.

Definitions

1. **Chief Administrative Officer (CAO)** means the person appointed as chief administrative officer of the Town of Westlock or his/her designate.
2. **Cyber Security Team (CST)** means the department responsible for overseeing, managing, implementing, and administering the Town's cyber strategy, including technology and policies.
3. **FOIP Act** means the *Freedom of Information and Protection of Privacy Act*, RSA 2000, Chapter F-25, as amended, or any statute enacted in its place.
4. **Mobile Device Management Tools** means software solutions that are used by the Town to manage and control mobile devices, such as smartphones and tablets within

the network.

5. **Removable Media Device** means any portable device that can be connected to an information system, computer or network to provide data storage.
6. **Technology Resources** means any and all technologies of the Town that produce manipulate, store, communicate or disseminate information. These resources include but are not limited to:
 - a. Desktop, portable and wireless computing devices and related peripherals (e.g. desk phones, printers, scanners, external and remote storage systems and devices, etc.);
 - b. Mobile computing devices including but not limited to notebook computers, laptops, tablets, cell phones, smart phones, air cards, push to talk radios and modems;
 - c. Internet and electronic communication services (e-mail, video streaming, instant messenger, voice mail, long distance and roaming, voice/text/data transmission, etc.);
 - d. Network infrastructure (e.g. switches, fiber optics cables, wireless networks and Wi-Fi access points, etc.);
 - e. Business systems, office productivity systems, utility and all other Town administered systems and related server and storage infrastructure;
 - f. Consumable goods used in the operation of these resources including, but not limited to DVD's, CDs, external storage devices, paper, USB memory sticks, etc.;
 - g. Data, information and other work products (e.g. computer programs, databases, spreadsheets, etc.) created/maintained in using these resources; and
 - h. Information – any collection of data that is processed, analyzed, interpreted, classified or communicated in order to serve a useful purpose, present facts or represent knowledge, an individual record or collection of records.

7. **Technology Resource Users (Users)** means someone who is authorized to and utilizes Technology Resources and includes but is not limited to Town employees, vendors, contractors, volunteers, and any other individuals with authorized access to and use of Technology Resources.
8. **Town** means the Town of Westlock
9. **Town's Network** means the Town's internal network and associated applications and services.

Principles

1. All Technology Resources acquired and managed by the Town, and the data, information and the work product (e.g. programs, databases, spreadsheets, etc.) created, received/downloaded from external sources and/or modified in the use of such resources, belong to the Town or its licensors.
2. Technology Resources are provided to improve productivity of Town business activities, delivery of citizen services, and enhance the effectiveness of communications.
3. Technology Resources must be used only for their intended purpose and in accordance with this policy.
4. Users of Technology Resources are required to use Technology Resources in an acceptable manner as defined in this policy.
5. Technology Resources may be used in, or accessed from, either corporate or non-corporate workspaces. Regardless of a User's location while using a Technology Resource, they must adhere to this policy.
6. Technology Resources must be used in activities in compliance with all applicable laws or regulations, including without limitation:
 - a. Those at the federal, provincial, or municipal level;
 - b. Those by way of international treaties;
 - c. Those of any foreign jurisdiction with authority;

- d. Those civil laws in force between vendor and purchaser of Technology Resources; and
 - e. Any and all Town policies.
7. Technology Resources are to be used in a manner consistent with the FOIP Act and related Town policies.

Procedures**1. Safeguarding Assets, Data and Information**

- a. Technology Resources are valuable assets, Users are expected to exercise reasonable care to prevent abuse or theft of Technology Resources.
- b. Technology Resources are to be used in a manner that safeguards the integrity and accessibility of data, information and the work product (e.g. programs, databases, spreadsheets, etc.) created, received/downloaded from external sources, and/or modified in the use of such resources.
- c. No User of Technology Resources should assume or operate under another User's electronic identity.
- d. Passwords should not be shared or revealed.
- e. Mobile computing device users are expected to ensure the devices they use do not unnecessarily pose security risks to the Town.
- f. Mobile devices may have Mobile Device Management Tools installed for security and supporting mobile devices across mobile operations.
- g. Removable Media Device Users are expected to ensure the devices they use do not pose security risks to the Town.
 - i. This includes information created, received, or downloaded from external sources and/or modified in the use of such resources.
 - ii. The information shall be completely deleted at the earliest opportunity after being transferred and stored on a Town Network drive to secure

back-up and recovery procedures of Technology Resources can be performed.

- h. Cloud solutions shall comply with this policy.
 - i. A risk-value assessment shall be completed and is subject to approval by the Town's CST prior to implementation.
 - ii. Town information stored at a vendor's location must be protected and comply with the Town's policies and guidelines.
 - iii. The Town's information is to be transferred back for storage on the Town's technology environment at the end of a contract with a cloud-solution vendor.
- i. When working in either corporate or non-corporate workspaces, reasonable care and safeguards are to be taken to protect the equipment, information, or network account to the same level as when working in the office.
- j. When leaving a computer, laptop or mobile device, technology resource users shall sign-out of their network account or lock the device.
- k. Users shall use secure access methods when working on Town documents from a non-corporate workspace.
- l. Emailing documents to personal email accounts is not permitted.

2. Monitoring

- a. The CST reserves the right to monitor, access, investigate, and audit the use of any and all Technology Resources.
- b. No User shall have any expectation of privacy as to their Technology Resources use.
- c. The CST reserves the right to remove, delete, confiscate or alter data, information and other work products (e.g. programs, databases, spreadsheets, etc.) found to be in violation of this policy.

- d. Users shall not expect privacy as to their internet activity.
 - i. The CST monitors and logs internet activity to assess and ensure policy compliance and to be alerted to possible technology risks.
 - ii. Internet activity may be reviewed to ensure compliance with this policy.
 - iii. At any time, with or without notice, incoming and outgoing messages may be monitored, reviewed, disclosed or assessed.

3. Personally Owned Technology Resources

- a. The Town does not manage, support, or reimburse for personally owned technology resources.
- b. When personally owned technology resources are used for remote work, devices must connect to the Town's network through secure remote access.
- c. Personal devices (e.g. portal electronic devices) shall not be connected to the Town's secured network without prior authorization by the CST or their designate.
 - i. Authorized personal devices and their contents may be visible to other Town Users when connected to Town computers, network or other Technology Resources.
 - ii. These devices may be subject to automated scans and data capture while connected.
- d. Town information shall not be stored on a personal device or on any computing device's local drive.
 - i. This includes, but is not limited to electronic communications, content and information.
 - ii. Town information shall be stored on a Town Network drive to ensure back-up and recovery can be performed.

4. Personal Devices

- a. Users are prohibited from removing or exfiltrating data from approved applications on personally owned devices. This includes, but is not limited to, copying, transferring, or sharing any data obtained through these applications without explicit authorization. Users must ensure that all data remains within the confines of the approved applications and is not stored or transmitted outside of these platforms.

5. Access Control

- a. Access control systems will be implemented to ensure that all data access and audits are conducted in accordance with established protocols. All users must adhere to the access controls set up for their respective roles, ensuring that data access is limited to authorized personnel only. Any audits or access to data must respect the confidentiality of user roles and the sensitive nature of the information.

6. Use of Town Technology Resources for Internet Access

- a. No User shall expect privacy as to their internet use.
- b. The CST monitors and logs all internet usage
- c. Internet activity may be reviewed to ensure compliance with this policy or other Town policies or as otherwise defined in Subsection 6, under the Principles header above.
- d. Access to the internet is provided to Users to enable them to carry out their job responsibilities.
- e. It is a breach of this policy to access websites that contain material that is in contravention of any other Town policy.
- f. The CST reserves the right to block any internet service that may pose a risk to the corporation and block access to some websites clearly not in keeping with this policy.
- g. The CST continuously monitors its technology systems to be alerted to possible

system risks and to assess policy compliance.

- h. Individual Users may be notified if their attempts to access blocked sites appear on corporate internet logs.

7. Use of Town Technology Resources for Electronic Communication Services

- a. No User should expect privacy as to their electronic communication services use.
- b. Incoming and outgoing messages may be reviewed, disclosed, accessed or monitored at the sole discretion of management, in the ordinary course of its business, at any time, with or without notice.
- c. Town credentials or identities shall only be used for Town business purposes. The use of Town credentials or identities to access or to participate in lone services for activities that are not Town business (e.g. services or citizenship activities) requires prior agreement of the Director or Manager.

8. Unacceptable Use of Town Technology Resources

- a. Unacceptable use of Technology Resources includes, but is not limited to, knowingly or intentionally doing or allowing any of the following:
 - i. Intercepting or altering data transmitted via Technology Resources.
 - ii. Violating terms of applicable software licensing agreement, including installing software without a license to do so.
 - iii. Using the Town's network to gain unauthorized access to any computer system data.
 - iv. Moving computer equipment and hardware (except for portable devices) without prior approval from the Town's CST.
 - v. Connecting unauthorized equipment to the Town's network.
 - vi. Attempting to circumvent the Technology Resources protection schemes.

- vii. Activities that will interfere with the normal operation of Technology Resources including computers, terminals, peripherals, and interconnected public Data/voice networks etc.
- viii. Using the Technology Resources for personal use that results in the Town incurring costs (e.g. purchase and download of games, ringtones, wireless TV, video and music downloads, premium messaging subscriptions, storing of personal data on Technology Resources etc.).
- ix. Unauthorized use, or infringement, or theft of data, equipment, or tangible or intangible property, or any intellectual property rights thereto.
- x. Distributing any communication that contains any form of material of a nature that is in contravention to any Town policy.
- xi. Assuming or operating under another User's electronic identity.
- xii. Sharing or revealing Town electronic identity or network account passwords and secure access codes.

9. Roles and Responsibilities

- a. The Town CAO is responsible for approving and supporting this policy
- b. The CST is responsible for providing strategic governance for technology, infrastructure and connectivity for the entire organization and implementation of business and Geographic Information Solutions (GIS) for all Town Departments.
- c. Directors, Managers and Supervisors are responsible for:
 - i. Making Users aware of this policy.
 - ii. Reviewing and approving Technology Resources purchases.
 - iii. Ensuring Technology Resource purchases are made in adherence to corporate guidelines and policies.

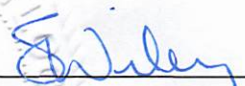
- iv. Providing Users with access to necessary training to use Technology Resources efficiently and effectively.
 - v. Informing senior management of any breach of this policy.
 - vi. Approving employee access to the Town's Technology Resources while vacationing or away on Town business.
 - vii. Monitoring wireless uses and charges.
 - viii. Updating Technology inventories and asset tracking in the event of staff changes (e.g. new hires, transfer, resignation, termination, or retirement).
 - ix. Taking appropriate action based on established procedures.
- d. Users are responsible for:
- i. Adhering to this policy.
 - ii. Becoming as proficient in the use of Technology Resources that are provided, as is necessary to fulfill work responsibilities.
 - iii. Promptly advising managers and supervisors if any inappropriate or improper message or material is received.
 - iv. Immediately advising CST of any loss or theft of Technology Resources.

10. Consequences of Non-Compliance

- a. Any use of Technology Resources that breaches this policy will be considered misconduct and will be reviewed.
- b. This may result in disciplinary steps being taken against the User, up to and including dismissal of employment, seeing restitution, commencement of civil action, criminal prosecution, or any combination thereof.



Mayor Jon Kramer



Chief Administrative Officer, Simone Wiley