

**Town of Saugeen Shores  
Corporate Policy**

<b>IT Acceptable Use Policy</b>	
<b>Department:</b> Corporate Services	<b>Prepared By:</b> Manager, IT
<b>Date of Passage:</b>	<b>Resolution Number:</b>
<b>Supersedes:</b> IT & Mobile Devices Policy	<b>Resolution Number:</b> 193-2013

**Purpose:**

This policy identifies responsibilities, requirements and provides guidance for all employees in the acceptable use of Town-owned computers, mobile devices, and all related components and resources.

**Policy:**

1. Background

The Corporation of the Town of Saugeen Shores is committed to promoting appropriate and responsible use of technology in order to enable a productive working environment for all Information Technology users.

2. Scope

2.1 This policy applies to all users of Town of Saugeen Shores Information Technology. For the purpose of this policy, where “employee” is referenced, it shall mean both permanent and temporary employees as well as elected officials.

3. General Acceptable Use

3.1. Every User needs to exercise good judgment on the appropriate use of the Town’s IT in accordance with legislation, the Town’s by-laws, corporate policies and related Standard Operating Procedures.

3.2. Utilization of the Town’s IT shall be for conducting Town business and shall not be used for any unlawful or prohibited purposes. Such purposes include, but are not limited to theft, fraud, slander, libel, defamation of character, harassment (sexual and non-sexual), pornography, stalking, identity theft, online gambling, spreading viruses, spamming, impersonation, intimidation, and plagiarism/copyright infringement.

3.3. IT resources are made available to users for business purposes. Occasional personal use may occur, however usage shall not be impact work productivity or interfere with work performance. Users are encouraged to ask their direct supervisor or the IT Help Desk if they have any questions regarding appropriate use.

3.4. Only those officially designated by the Corporation shall use social media to speak

on behalf of the Corporation. Refer to the Social Media Policy for further information.

- 3.5. External social media channels should not be used for internal business communications among fellow employees. Individuals are to exercise personal responsibility whenever they use social media, which includes not violating the trust of those with whom they are engaging. Individuals should never use social media for covert advocacy, marketing or public relations.

#### 4. Access to Information Technology Resources

- 4.1. Users are responsible for the security of account(s) under their control and must keep their password secured at all times. Users shall not share their account(s) or password information with anyone, including other employees, third-parties, family or friends.
- 4.2. The storage and use of personal multimedia, files and/or tools on Town's infrastructure is prohibited.
- 4.3. All reasonable efforts must be undertaken to prevent loss, damage and theft of Town IT assets and data. If it is evident that damage was due to negligence, the employee may be personally liable for the replacement cost.
- 4.4. All users must promptly report to the IT Help Desk any theft, loss, or damage to assigned IT assets.
- 4.5. Only removable storage provided and authorized by IT staff are allowed (i.e. USB key, external drives).

#### 5. Data and Software

- 5.1. All systems and their content are the property of the Corporation of the Town of Saugeen Shores (the "Corporation"). This includes all applications, documents, Emails, spreadsheets, databases, etc., developed using corporate equipment and/or software.
- 5.2. Only software and/or hardware that have been approved by the Corporation shall be used by employees.

#### 6. Freedom of Information

- 6.1. All electronic documents, which are created by or with the Corporation's computers or network, including internet related systems are records for the purposes of the Municipal Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. M.56 (MFIPPA) and may be a public record for the purposes of this Act.
- 6.2. The use and disclosure of e-mail messages shall be covered under the provisions of the MFIPPA, R.S.O. 1990, c. M.56 (MFIPPA).
- 6.3. Email messages shall be considered to be machine-readable records owned by the Corporation, for the purposes of MFIPPA.

## 7. Filtering/Monitoring

- 7.1 For security, compliance, and maintenance purposes, authorized staff may monitor and audit equipment, systems, and electronic communications. Making use of Town resources implies the user's consent to monitoring for such purposes.
- 7.2 All users covered by this policy should bear in mind that internet sessions are likely not private. Where the Town discovers activities that conflict with the law or this policy, usage records may be retrieved and used for documentation purposes.

## 8. Mobile Devices

### 8.1. Use of Personal Equipment for Work Purposes

Employees who require mobile devices in the performance of their job duties shall be provided an appropriate Town-owned device. Information Technology services shall endeavor to provide the most effective and cost-efficient solutions to ensure appropriate mobile devices are provided to staff.

### 8.2. Mobile Device General Information

Town-owned mobile devices shall be managed via a Mobile Device Management (MDM) platform to ensure compliance with data protection and security requirements.

## 9. Generative Artificial Intelligence (A.I.)

- 9.1. Employees may only use Generative A.I. software or applications to produce work for the Town that are approved for use. As of the effective date of this policy, the Town has approved Microsoft Copilot for use by employees, provided it is used in compliance with this policy.
- 9.2. Employees must be able to identify where information in their output has come from. Generative A.I. should only be used as a secondary source. Employees are responsible for finding the primary source and verifying information. If employees are unable to verify the accuracy of the output using the requested source information, they may not rely on Generative A.I. output or trust its accuracy.
- 9.3. Employees must continue to work with all departments to ensure that Generative A.I. outputs are consistent with the Town's policies, procedures, and guidelines. Examples include contracts, public-facing and/or stakeholder promotional materials, brand identity, staff reports, coding, etc.
- 9.4. Employees remain responsible for their final work product and its adherence to all Town policies and procedures.
- 9.5. Employees should ensure when using A.I. that the final product aligns with [Ontario Bill 194](#) (Strengthening Cyber Security and Building Trust in the Public Sector Act) wherever possible. This can include a comment, footnote or watermark identifying the use of A.I.

## 10. Disciplinary Action

- 10.1 Violations of this policy may result in disciplinary action according to applicable Town of Saugeen Shores policies, up to and including suspension or termination of

employment with cause.

11. Acknowledgment

I acknowledge that I have read, understood and agreed to abide by the Town of Saugeen Shores Information Technology Acceptable Use Policy.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date