Statement of Policy and Procedure			
Department:	Corporate Services	Policy No.	**119**
Section:	Information Technology	Issued:	June 1, 2026
Subject:	**Information Technology Acceptable Use Policy**	Effective:	June 1, 2026
Council Resolution # and Date:	Council Resolution No. 0161 dated June 1, 2026	Replaces:	Policy No. 30 Policy No. 57
Issued by:	Corporate Services Department	Dated:	June 1, 2026
Approved by:	Kiley Bear, Director of Corporate Services		

1 POLICY

1.01 The City of Prince Albert provides information technology (IT) resources including but not limited to computers, mobile devices, servers, networks, software, cloud services, and communication tools to support effective delivery of municipal services and operations. Use of these resources must be responsible, professional, lawful, and aligned with City expectations.

1.02 The City reserves the right to monitor, audit, log, and access the use of its IT resources for purposes including security, compliance, operational integrity, and investigation. While limited incidental personal use may be permitted, users should be aware that their use of City IT resources may be monitored or accessed in accordance with applicable legislation and City policies.

1.03 All users of City IT resources including employees, contractors, volunteers, elected officials, and third-party service providers must comply with this Policy, related guidelines, and all applicable laws, licensing terms, and contractual obligations.

1.04 Users are responsible for protecting City systems and data by following cybersecurity requirements, including safeguarding credentials, avoiding unsafe online behaviour, and maintaining vigilance against cybersecurity threats.

2 PURPOSE

2.01 The purpose of this Information Technology Acceptable Use Policy is to establish clear, consistent, and enforceable rules for the use of City IT resources to protect the integrity, security, reliability, and confidentiality of City information and systems, and to safeguard City assets and public trust.

2.02 This Policy helps ensure that IT resources are used efficiently and responsibly, minimizing risk arising from misuse, unauthorized access, data breaches, and compliance violations.

2.03 The Policy provides guidance for acceptable use of IT resources, clarifies prohibited behaviours, supports the City's information-security posture, and ensures transparency with respect to monitoring, data handling, and accountability.

3 SCOPE

3.01 This Policy applies to all users with access to City IT resources, including full-time, part-time, temporary and contract employees; volunteers; elected officials; third-party contractors and consultants; and any individuals or entities granted access to City systems or networks.

3.02 This Policy applies to all IT resources owned, leased, licensed or managed by the City of Prince Albert including desktops, laptops, mobile devices, servers, storage devices, networks, cloud services, software, email, Internet access, and communication systems.

3.03 This Policy also applies when users access City IT resources through personal or remote devices (e.g., under a Bring Your Own Device (BYOD) arrangement), in accordance with the City's BYOD Guidelines. To protect City information, the City may implement controls such as access restrictions, device management tools, and the ability to remove City data from such devices where necessary.

3.04 This Policy does not apply to private, personal devices and systems used exclusively for personal reasons that do not interact with City systems, provided such use is entirely separate from City business, data, and networks.

4 RESPONSIBILITIES

4.01 Users are responsible for adhering to this Policy and for safeguarding their

access credentials, reporting lost or stolen devices, and immediately reporting any suspected security incidents or policy violations.

4.02 Managers and supervisors are responsible for ensuring that staff under their supervision are aware of this Policy, understand its requirements, comply with its provisions, and receive appropriate guidance and training.

4.03 The Information Technology Department is responsible for implementing and maintaining the technical infrastructure, security controls, monitoring, logging, and enforcing compliance with this Policy.

4.04 The City Clerk (or designate) is responsible for ensuring that use of IT resources and monitoring practices comply with applicable privacy legislation and for responding to data access or disclosure requests.

5 DEFINITIONS

5.01 “City” means City of Prince Albert

5.02 “City IT Resources” means all hardware, software, networks, cloud services, communication tools, and data storage systems owned, leased, licensed, or managed by the City.

5.03 “User” means any individual authorized to access City IT resources (employees, contractors, volunteers, elected officials, third-party service providers).

5.04 “Acceptable Use” means use of City IT resources in a manner that is lawful, ethical, professional, consistent with job responsibilities, compliant with this Policy and related guidelines, and respectful of City systems, data, and public trust.

5.05 “Malicious Software (Malware)” means software or code designed to damage, disrupt, or gain unauthorized access to City systems, data, or networks (e.g., viruses, ransomware, spyware, worms, trojans).

5.06 “Unauthorized Use” means any use of City IT resources not permitted by this Policy, including use that violates laws, licensing terms, City policies, or ethical standards.

5.07 “City Systems” means any municipal information technology resource, including networks, applications, email systems, servers, cloud services, and communication tools.

5.08 “BYOD (Bring Your Own Device)” means a personal device used by a user to access City systems, networks, or data under the terms of the City’s BYOD Guidelines.

5.09 “Sensitive Data” means any information that is protected under privacy, confidentiality, or regulatory requirements (e.g., personal information, financial data, health information, law-enforcement related data).

6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

6.01 Bring Your Own Device (BYOD) Guidelines

6.02 Privacy and Confidentiality Policy

6.03 Any other applicable City policies (e.g., Code of Conduct, Privacy, and HR)

6.04 Information Technology Investigation – Standard Operating Procedure (SOP)

6.05 Artificial Intelligence Use Guidelines

7 PROCEDURES

7.01 Authorized Use and Acceptable Behaviour

a) Users must access and use City IT resources only for authorized City business. Incidental personal use is permitted only if: it does not interfere with work duties, does not impose additional cost on the City, does not involve prohibited content or activities, and complies with all provisions of this Policy.

b) Users must protect their login credentials, not share accounts or passwords, and ensure devices are locked or logged out when unattended.

c) Only software, applications, and services approved by the IT Department may be installed or used. The use of unauthorized third-party services to store, process, or transmit City information is prohibited.

d) Sensitive Data must only be stored, transmitted, or processed using approved City systems, services, or encrypted methods.

Personal storage or personal cloud services for Sensitive Data are prohibited.

7.02 Prohibited Uses

Users shall not use City IT resources for any of the following:

a) Illegal activities, including but not limited to fraud, harassment, hate speech, discrimination, or copyright infringement.

b) Installing or using unlicensed software, malicious software, or software that violates licensing agreements.

c) Bypassing or disabling security controls, firewalls, or network protections.

d) Unauthorized access to or disclosure of City sensitive data, including any sharing of credentials or enabling access by unauthorized individuals.

e) Using City systems for personal financial gain, commercial ventures, political campaigning, or mass unsolicited communications (spam).

f) Storing, downloading, or distributing pornographic, objectionable material, offensive, or unlawful content.

g) Excessive personal use that interferes with job duties, performance, or imposes costs on the City.

7.03 Security, Monitoring, and Auditing

a) The City may use electronic monitoring tools such as system logs, network monitoring, device management tools, access controls, and related technologies to protect City systems, to ensure security, support operational integrity, and investigate suspected misuse or misconduct.

b) The City reserves the right to monitor, log, audit, and review use of its IT resources, including email, network traffic, device activity, cloud usage, and stored data.

c) Monitoring and auditing will be conducted in compliance with related policies, privacy obligations, and legal requirements.

d) Users must immediately report suspected security incidents, data breaches, lost or stolen devices, or unauthorized access to their supervisor or IT Department.

e) Any suspected or confirmed privacy breach involving personal information must be immediately reported to the City Clerk (or designate), in accordance with the City's privacy breach response procedures and applicable legislation.

f) Requests by Managers or Supervisors to access or review a specific user's IT activity, account, or data must be supported by a legitimate business reason and approved by Human Resources and the City Clerk's Office. All requests must follow established procedures, and any access will be limited to what is reasonably necessary and conducted in accordance with applicable legislation and City policies.

7.04 Data Retention and Disposal

a) Data stored on City IT resources will be retained according to the City's Records Retention and Disposal Schedule.

b) Storage of Sensitive Data must follow classification, encryption, and access controls consistent with the City's data governance standards.

c) Information obtained through monitoring may be used for system administration, security, compliance, performance management, or investigation of policy or legal violations. Monitoring data will be retained only as long as necessary and handled in accordance with the City's records retention, privacy, and information-management requirements.

7.05 Enforcement and Consequences

a) Violations of this Policy may result in disciplinary action, suspension or revocation of access rights, termination of employment or contract, and/or legal action.

b) The IT Department may suspend access to systems or accounts pending investigation of a suspected violation.