

	Acceptable Use of Information Technology Assets Policy	
	Section No: 2.12	
	Category: Workplace Conduct and Compliance Policies	
	Resolution Number: 257-2026	
	Effective Date: September 1, 2026	
	<i>Supersedes: former Section 39, Resolution 2023-106 – November 1, 2022</i>	
	Next Review Date: September 1, 2028	
Responsible Office: Information Technology		
Policy Applies to:	☒ All City employees (Full-time, Part-time, LSEs, temps, etc.) ☐ All City and School Employees	☒ Full-Time employees only ☐ Other: _____

Relevant Definitions

N/A

Policy

This policy is to inform users of the city’s information technology assets of what information technology uses are permissible and what uses are prohibited. Compliance with this policy drives the city’s ability to protect government services, government employees, and the citizens of Kingsport. This policy applies to all city employees and assigned designee(s) (hereinafter “Users”) utilizing city-owned, installed, controlled, or provided information technology assets (*i.e.* device(s), data, internet access, and network).

1. Access and Use

1.1. User Access: All User access to information technology assets:

- shall be approved by the department head;
- shall be limited to the information technology assets necessary and appropriate for the User to perform the job duties and function to which they are assigned.

1.2. Access from External Devices: A User shall not access sensitive information from a device other than one issued to the User by City or approved for use by the Information Technology department.

2. Security

2.1. Use of Passwords or other authenticating information: Users are responsible for safeguarding all authentication information and credentials, including passwords, passphrases, PINs, authentication tokens, security keys, smart cards, and physical access cards. Authentication information and credentials must remain confidential and may only be stored in IT-approved credential management solutions. They must not be written down in an unsecured manner, stored near the associated device, maintained in

unapproved locations or applications, or shared, loaned, or otherwise disclosed to any other person, including managers, supervisors, direct reports, coworkers, or contractors.

2.2.

2.3. Virus Protection.

2.3.1. If a User has any reason to suspect material may be infected by a virus or other malware, the User shall immediately contact the Information Technology help desk so that the material can be virus-scanned. Users shall not knowingly or negligently store, send, or create destructive programs, including any virus, self-replicating code, or any other program that operates in a similar fashion. Users shall not disable or modify the existing city supported anti-virus software.

2.4. Prohibited Acts

2.4.1. Personal Use: Information technology assets are intended for business purposes. Personal use shall be permitted when such use does not:

- interfere with the User's work performance;
- interfere with any other User's work performance;
- unduly impacts the operation of the city and/or its Information Technology;
- violate any law, rule, regulation, court order; or
- violate any provisions of this policy, or any other city policy, standards, or practices.

Users must use information technology assets in a professional, ethical, and legal manner regardless of whether such use is personal or business-related.

2.4.2. Unauthorized System Access: The ability to read, alter, or copy a file belonging to another. User shall not imply permission to access that file. Use of information technology assets to obtain unauthorized access to the computer systems of other individuals, companies, or entities (*i.e.* "hacking") is strictly forbidden.

2.4.3. Purchasing Computer Hardware: The Information Technology department is the sole approving authority for purchasing computer hardware, software, cell devices, tablets, and technical services for the City of Kingsport. This includes laptops, desktops, tablets, mobile computers, printers, storage devices, servers, cloud services, televisions, desk phones, monitors, power supplies, cables, and peripherals. A department or individual is required to request approval for such items through IT.

2.4.4. Proper Storage of City Information: Critical business information shall be stored on network drives located on city supported servers that are backed up and where access to this information can be secured. The storage of information of the city to third-party hosted network storage areas shall not be allowed without prior approval from the Information Technology department.

3. Privacy

3.1. Acknowledgement and Consent to “No Expectation of Privacy”:

Except as otherwise provided by applicable law, users shall not have an expectation of privacy in any information they create, store, send, or receive on information technology assets. The city retains the right to monitor all aspects of its information technology assets, including, without limitation, internet sites visited by users, monitoring chat groups and newsgroups, reviewing materials downloaded or uploaded electronically, and reviewing files and email created, stored, or received by a User.

4. Email Guidelines

4.1. Mass Email Distribution: Except where necessary for legitimate City business purpose, the transmission of email to a general, non-specific audience of all City Users is prohibited. Requests to send emails to all City employees must be approved by the department head, and, where necessary, by the Human Resources Department. Requests to send department wide emails must be approved by the applicable department head.

4.2. Signature Language: Use of any email footer or signature block requires approval of the Public Information and Communications Department.

5. At Work Network Access: At work network access, wired or wireless, to a City supported network, except when specifically provided for public use, shall be limited to City issued and supported devices or approved user owned devices. Employees shall be aware of the following:

A. Public Records: Pursuant to Tenn. Code Ann. § 10-7-503, *et seq.* procedures for public records is governed by City of Kingsport **Public Records Policy**. Users should be aware that anything transmitted or stored on devices may be a public record.

B. Noncompliance: Noncompliance with this policy may constitute a legal risk; an organizational risk in terms of potential harm to employees or citizen security; a security risk to the city’s network operations and the User community; and/or a potential personal

liability. The presence of unauthorized data in the network could lead to liability on the part of the city, as well as the individuals responsible for downloading/sharing it.

Consequences of Policy Violation

Violations of this policy may be subject to disciplinary action, up to and including termination of employment.

Related Information or Procedures:

N/A

Other Provisions:

Nothing in this policy should be construed to conflict with or supersede state or federal law, or as interfering with the constitutional rights of employees.

While the city is committed to the principles embodied in this policy, the policy itself is not intended to state contractual terms and does not constitute a contract between the city and its employees. Furthermore, this statement constitutes ONLY the policy of the city. A finding of a violation of this policy does not mean that the conduct violates state and/or federal laws.

Contacts

The Human Resources Office can address questions regarding this Policy: phone: (423) 229-9401, email: HROffice@kingsporttn.gov