



City of Elizabeth City

Acceptable Use of Information Technology

Administrative Policy (AUP)

February 2025

Introduction:

This Acceptable Use Policy (AUP) outlines guidelines and expectations for the use of City of Elizabeth City's IT resources, including but not limited to computers, networks, internet access, email systems, and other collaboration tools. All users are required to adhere to this policy to ensure the efficient, secure, and ethical operation of City systems.

I. Authorized Use

City technology resources are provided for conducting City business. Acceptable use includes, but is not limited to, the following activities:

- Conducting City-related business activities and communications.
- Accessing resources for professional development, research, and training that support City functions.
- Communicating with City departments, contractors, and external partners for City business.
- Using technology resources to fulfill the duties and responsibilities of a City role.

Users must make reasonable efforts to protect City technology and data from unauthorized access, use, and disclosure.

II. Prohibited Activities

The following activities are prohibited and may result in disciplinary action, up to and including termination of system access and other measures deemed necessary to maintain security.

- **Violation of City Policies:** Engaging in activities that violate the City's Standards of Conduct or policies.
- **Harmful Activities:** Using City resources to harm others, such as spreading slander or causing damage to City property.
- **Taglines:** The use of non-approved taglines in any communication on City technology.

- **Malicious Activities:** Creating or distributing viruses, malware, spyware, or any other harmful software.
- **Unauthorized Access:** Gaining unauthorized access to systems or passwords, circumventing security measures, or revealing your password.
- **Political Use:** Using City resources for partisan political purposes, including circulating material for political candidates.
- **Illegal Activities:** Committing crimes such as fraud, identity theft, or distributing illegal material such as child pornography.

III. Definitions

For the purposes of this policy, the following definitions apply:

- **City Technology:** All IT resources, including networks, hardware, software, systems, and devices (such as cell phones, tablets, and personal digital assistants) provided, owned, or operated by the City of Elizabeth City or its contractors for use in city business. This also includes technology provided by third-party service providers.
- **Device:** Any device capable of receiving or transmitting data to or from city information systems, including computers, mobile devices, and storage media.
- **Electronic Records:** Computer-based records, including emails, text messages, voice messages, images, web pages, and other machine-readable records created, stored, sent, or received using city technology. These records may be considered public under applicable laws, including the North Carolina Freedom of Information Act.
- **Information:** Any data, in any form, created, contained in, or processed by city information systems, networks, or storage media.
- **Information Systems:** Computer-related equipment and components capable of managing, transmitting, receiving, or storing information. This includes devices like USB drives, laptops, servers, cloud storage, and other IT infrastructure, along with the software and data used to process or store information.
- **Internet:** A global network of interconnected computers and networks used to share information, accessed by various organizations, including governments, businesses, and educational institutions.
- **Intranet:** A private network used by an organization for internal communications and information sharing, typically based on the same technology as the internet but accessible only to authorized users.
- **Password:** A string of characters used to authenticate a user's identity, granting or denying access to systems and data. Strong passwords are long and complex, avoiding easily guessed terms or personal information.
- **Server:** A system that provides services to other systems (clients), typically hosting multiple services and applications for network use.
- **Third-Party Service Providers:** External firms providing services to the City, such as those offering telecommunications, data storage, and transmission services for use by City employees.
- **User:** An individual or automated process authorized to access City IT resources in accordance with the City's procedures and rules.

- **Web Page:** A document on the World Wide Web, identifiable by a unique Uniform Resource Locator (URL).
- **Website:** A location on the World Wide Web, consisting of a homepage and additional pages or documents, accessible via a unique URL.

IV. Email and Electronic Messaging Use

- **Sender Identity:** All messages sent via City email or messaging systems must contain the sender's name and must not attempt to mask or impersonate others.
- **Reasonable Use:** Users are responsible for the content of all text, audio-video, or images sent over City communication systems.
- **Acceptable Uses of City Email:**
 - Communicating information related to City work, programs, policies, or training.
 - Administering grants or contracts for City programs.
 - Professional development communication.
 - Discussing City-related advisory, standards, or professional society activities.
 - Announcing new laws, procedures, or services related to City business.
 - Incidental personal use is allowed, but users should clarify that they are not representing the City unless authorized, using a disclaimer such as: "The opinions expressed are my own, and not those of the City of Elizabeth City."

V. Data Security and Privacy

- **Confidentiality:** Users must comply with laws and City policies regarding the confidentiality of personal, tax, and employee information.
- **Secure Communication:** Confidential information should only be sent to authorized recipients.
- **System Security:** Users should implement security measures, such as password protection, and lock or log off their systems when not in use.
- **Data Protection:** All users must follow the City's guidelines and Federal laws for handling sensitive data.

VI. Security and User Responsibility

- **Passwords and Access:** Users must create strong, secure passwords and must not share their credentials with anyone.
- **Reporting Security Breaches:** Any suspected security breach should be reported to the IT department immediately.
- **Device Configuration:** Altering City device configurations or bypassing security measures without written authorization is prohibited.
- **Unauthorized Devices:** Personal devices should not connect to the City network without prior approval from the IT Department.

VII. Prohibited Use of Information Technology

Certain activities are prohibited when using City information systems, applications, data, and resources, including but not limited to:

- **Inappropriate Content:** Transmitting offensive, discriminatory, or sexually explicit content.
- **Illegal Copies:** Creating, using, or distributing pirated software or copyright-protected material.
- **Disruptive Behavior:** Intentionally wasting IT resources or creating network disruptions.
- **Harassment and Abuse:** Engaging in harassment, intimidation, or discriminatory behavior.
- **Personal Gain:** Using City resources for personal financial gain, including activities like crypto mining or gambling.
- **Spamming:** Sending unsolicited, fraudulent, or hoax messages.

VIII. Circumventing Security Controls

Any attempt to bypass or disable security controls (e.g., sharing passwords, disabling antivirus software, or creating unauthorized network connections) is a violation of this policy and may lead to disciplinary action.

IX. Illegal Activities

The City's network and systems must not be used for illegal activities. If suspected illegal activities are detected, they may be reported to the appropriate authorities.

X. Pornography

Users are expressly prohibited from accessing, viewing, downloading, storing, or distributing pornography or sexually explicit content on any City-owned or networked device. This includes, but is not limited to, computers, laptops, tablets, and mobile devices, whether connected to the City's network or not. Violations may result in disciplinary action, up to and including termination.

XI. Termination of Access

Violations of this policy may result in termination of access to City systems and resources.

- **Termination of Access:** If necessary, the Department Head, Chief Information Officer, or Director of Human Resource Management may terminate an employee's access to City systems.
- **Separation from the City:** Upon separation from the City, employees must return all City-owned equipment and their access to City systems will be revoked.

XII. Reporting Violations

- Users who suspect violations of this policy should report concerns to their supervisor, the Department of Human Resource Management, or the IT Department.
- For questions related to acceptable use, employees can contact the IT Department at (252) 621-1794, and for disciplinary matters, they should contact the Department of Human Resource Management at (252) 621-7356.

Acknowledgment

By using City of Elizabeth City's IT resources, users acknowledge they have read, understood, and agree to comply with this Acceptable Use Policy. Violations may result in disciplinary action, up to and including termination. If you have any questions or need clarification regarding this policy, please contact the IT Department.