INFORMATION TECHNOLOGY POLICY

Policy Title:	702 – ELECTRONIC COMMUNICATIONS	Policy Number: APR 702
Effective:	July 13, 2022	
Supersedes:	Revision November 2012	
Approval:	Tom Shewchuk	Page 1 of 6

1. Scope

☒ Full-time
☒ Part-time
☒ Temporary/Contract
☒ Salaried
☒ Union
☒ Independent Contractors
☒ Visitors and Vendors
☒ Volunteers/Unpaid Interns

Employees who are covered under the provisions of a collective bargaining agreement will follow the standards as contained in their respective contracts if this policy conflicts with the language in the contract.

This policy is applicable City-wide. All users of City electronic communication systems are expected to comply with this policy as a condition of continued employment or contracted services.

The provisions of this Policy are subject to, and may be superseded by (in the event of a conflict), relevant provisions of applicable collective bargaining agreements between the City and the various collective bargaining associations of the City

2. Purpose

The purpose of this policy is to define the acceptable use standards and control requirements for City electronic communication systems, including but not limited to: email, instant messaging (IM), and text messaging.

2.1 Rationale

Electronic communications, including email, instant messaging (IM), and text messaging, can be intercepted, forwarded, printed, or stored by others.

Under certain conditions, electronic communications remain retrievable when a traditional paper communication would have been discarded or destroyed in the normal course of business. Employees must be aware that topics covered in electronic communications sent through City systems could disclose sensitive or inappropriate information which could breach City security measures, cause the City public embarrassment, or financial loss.

3. Responsibilities

3.1 Electronic Communications users are responsible for:

- Being familiar with and fully complying with this policy
- Exercising due care when using City electronic communication systems
- The management, retention, disposal and classification of their electronic communications consistent with adopted City record retention policies

3.2 Management is responsible for:

- Periodically reviewing the electronic communications accounts that they are responsible for and requesting that ITSU remove those accounts that are no longer required
- Alerting Human Resources of the termination of an employee and requesting that their electronic communications accounts be disabled and if necessary, their contents retained and/or access transferred to the appropriate authorized City personnel
    - Human Resource management is responsible for informing ITSU of the requested changes via a Helpdesk ticket.

3.3 ITSU is responsible for:

- Classifying electronic communications users with the correct employment type
- The management, retention and disposal of backup or archived electronic communications on City servers

3.4 Failure to comply with this policy is a violation of the City's Employee Standards of Conduct policy and may lead to:

- Revocation of system privileges
- Disciplinary action according to the City's Progressive Discipline policy

3.5 Failure to comply with this policy by a contractor using City technology resources may be considered grounds for breach of its contract and revocation of system privileges.

4. Policy

- City electronic communication systems, including but not limited to: email, instant messaging (IM), and text messaging are provided for use by City employees (or other personnel) for legitimate City business purposes.
- Personal accountability is mandated for user electronic communications accounts. Passwords used to access electronic communications must not be shared.

4.1 Acceptable Use

- Personal non-City electronic communications accounts must not be used for the generation of City records.
- Email communications should always be handled inside of City provided a2gov.org email systems and City business should not be conducted in outside email systems.
- Accessing, reproducing, displaying, distributing or storing any materials that are sexually explicit, obscene, defamatory, harassing, illegal, or otherwise inappropriate is strictly prohibited.
    - An exception is made for Law Enforcement, 15th District Court, City Attorney and Human Resources personnel only when handling this type of material is required in the course of their official City duties.
- All City electronic communications must be consistent with the City's HR Employee Standards of Conduct policy.
- Without prior written authorization from the City Administrator and/or City Council, City electronic communication systems must not be used for charitable fund raising campaigns.
- City electronic communications may not be used for political advocacy efforts, religious efforts, private business activities, distributing chain mail, propagating hoaxes, or other purpose that could cause embarrassment to the City or otherwise adversely affect its interests or violate federal or state laws.
- News feeds, email lists, RSS feeds, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both City business and the duties of the receiving user. Users are reminded that the use of City technology resources must never create the appearance or the reality of inappropriate use.
- Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is prohibited. The user name, electronic communications address, organizational affiliation, and related information included with electronic communications must reflect the actual originator of the messages or postings.
- With the exception of City-sanctioned electronic communications systems (IT system maintenance notices, list servers, etc) that are

intended to be anonymous, sending anonymous electronic communications is strictly prohibited.

4.2 Electronic Communications Content

- Offensive material must not be forwarded or redistributed to either internal or external parties, unless this forwarding or redistribution is in connection with your official City-assigned work duties or is being sent to the City Human Resources Service Unit or City Attorney's Office in order to assist with the investigation of a complaint.
- Electronic communications content should not be altered and then forwarded without the permission of the originating sender. If content is altered to remove sensitive information, it must be clearly indicated in the new message. Altering the content to change the intention of the originator is strictly prohibited.
- Despite the best efforts of the City, electronic communications systems may deliver unsolicited messages that contain offensive content. The City is not responsible for the content of material viewed, downloaded or received through the Internet.

4.3 Electronic Communications Management

- Database files, used by City electronic communication systems are archived on City servers for disaster recovery purposes and will be deleted at periods chosen by ITSU but not to be less than six weeks.
- Electronic communications content which documents a decision, action or transaction is considered an official City record and must be managed and retained according to the City's Records Retention policies.
- Electronic communications inboxes are not intended to be repositories for official City documents or other important business-related correspondence. Users must regularly move these correspondences to word processing documents, databases, or other electronic file storage areas located on the City Network that are intended for storing official documents.

4.4 Malware and Viruses

- All email that leaves or enters the City networks will be scanned for malware (viruses, worms, etc.) by ITSU.
- Users must not click links or download attachments contained within electronic communications coming from unknown sources. If assistance is needed to determine an electronic communication's legitimacy, contact ITSU Security and Controls through the Helpdesk.

4.5 Phishing (Fraudulent) Messages

- Users must immediately delete “phishing” (fraudulent) electronic communications messages that ask for sensitive information. If assistance is needed to determine an electronic communication’s legitimacy, contact ITSU Security and Controls through the Helpdesk.
- Users must not click links or download any attachments within phishing (fraudulent) electronic communications messages.

4.6 Encryption

- By default, electronic communication is an unsecure platform and is not suitable, by itself, for sending sensitive information. An electronic communications message assumes the classification of the data contained in the message and therefore sensitive information must only be sent via electronic communication if it is appropriately protected using the City’s encryption services.
- ITSU will identify and provide a method for encrypting sensitive outgoing electronic communications that require additional protection because of their content.

4.7 Electronic Communications Forwarding

- Automatically forwarding electronic communications from a City electronic communications account to a public electronic communications system is prohibited without written permission from ITSU since the contents of the electronic communications, including attachments, can be forwarded, intercepted, printed, and stored by unauthorized parties.
- ITSU cannot guarantee that public electronic communications systems are private with access limited to only the intended recipients(s).

4.8 Broadcasts and Alerts

- ”All user” email broadcasts or mass electronic communications are not permitted except by permission of the City Administrator.

4.9 Delegate Authority

- Electronic communications must not be read or sent from another user's account, except under proper delegate arrangements.
- Generic User IDs should be used for electronic communications only when it is impractical to use personal User IDs. When a generic User ID is used, all other users of the generic account must be given delegate access to the functions that they require.

4.10 Third Parties

- Vendors wishing to communicate electronically with the City must use their own electronic communications systems.
- Contractors operating in direct support of City business operations may use City electronic communications systems. In these cases, requests for use of City electronic communications systems and deviations from prescribed functionality must be reviewed and approved by ITSU management with recommendation from their contract administrator.