River Heights City

Electronic Mail Use Policy

PURPOSE

The intent of this policy is to provide and explain the requirements, guidelines, and best practices for the use of electronic mail (email) that complies with the Utah Government Records Access and Management Act (GRAMA) and records retention schedules approved by the State Records Committee.

BACKGROUND

- The need to properly manage email messages and systems is the same as for other recordkeeping systems, which is to ensure compliance with State law and City ordinance concerning the creation, retention of, and access to public records.
- Emails created or received by employees, agents, or representatives of River Heights City are subject to GRAMA and therefore must be managed and maintained appropriately.

OPEN MEETING LAWS

Elected and appointed officials shall comply with all open meeting laws under UCA Title 52, Chapter 4 and shall refrain from creating situations that violate such law.

- Documents and email created or received on City-owned computers or sent over City-run networks are the property of the City.
- Email related to City business is recognized as official correspondence. Whether printed or not, it is subject to the same policies, rules, and procedures, and must be treated in the same manner as any City correspondence sent or received in printed format.
- Deletion of emails will not delete them from the backup system.
- Elected Officials are discouraged from using a personal email account from an outside email provider to conduct city business as it can be difficult to maintain appropriate records. However, if the elected official chooses to use a personal email account to conduct city business, then it is subject to the policy and procedures outlined above and examination for matters related to human resource personnel matters, litigation disclosures, forensic analysis, and information requests under the Government Records Access Management Act (GRAMA).

PRIVACY & SECURITY

- The City reserves the right to monitor, access, retrieve, read and disclose all information and material - whether business related or personal - that is created, sent, received, accessed or stored on its electronic resources, including emails and texts.
- The City may access such information and material at any time without any notice to the User. Users, through the internet, or other computer networks, cell phones or other Electronic

Communications systems (ECS), expressly waive any right of privacy in anything they create, store, send or receive on any/all City issued ECS or workstation equipment and systems (including but not limited to desktop computers, laptops, terminals, cell phones, etc.).

- Except for the City's right to retrieve, review and disclose messages as described above, all messages created, sent, received, or stored are considered to be confidential and as such are to be read only by the recipient or at the direction of the addressed recipient.
- Employees shall use caution when opening any emails or attachments from senders who are not known to the employee to avoid inadvertently downloading viruses or malware.
    - *Training*: Employees are required to go through the Phishing Trainings which are offered to them.
    - *Compromised Email Accounts:* If an employee suspects that their email account is compromised, they must notify the City IT department immediately.
    - *Detecting Malicious Content:* If there is any unusual feature of an email, or if it looks abnormal in any way, it is recommended employees do not download any attachments and notify IT. Under no circumstances should employees forward an email that is suspicious.
    - *Removing Malicious Emails and Content:* Malicious emails and emails with hazardous content should be deleted from email inboxes and from the deleted items folder so that they no longer exist on the device. If malicious content is suspected to already be on the device, employees should contact IT.
- Except as provided for herein, no employees shall access emails of another employee without permission from that employee.
- Mobile devices with email applications in use must at minimum use passcode security preventing unauthorized access to the device.

APPROPRIATE USE

All email and text messaging users are expected to know the difference between appropriate and inappropriate use of these communication technologies. This appropriate use policy applies to anyone who is representing River Heights City.

- Unacceptable Uses of the River Heights City Electronic Mail System:
    - Any illegal purpose
    - Transmitting threatening, obscene, or harassing materials or messages
    - Distributing confidential City data and information
    - Interfering with or disrupting network users, services, or equipment
    - Private purposes, such as marketing or business transactions
    - Installing copyrighted software or computer files illegally
    - Promoting religious and political causes.
    - Unauthorized not-for-profit business activities.
    - Private advertising of products or services.
    - Modifying, obtaining, or seeking information about files or data belonging to other users, without explicit permission to do so.

- Alternatives to Email for Work-related Activities - Email is not appropriate for transmitting and documenting the following work-related activities:
    - Information on impending personnel actions, such as employee disciplinary matters and performance evaluations.
    - Confidential information or information that can be used to breach personal privacy (such as Social Security numbers or medical information).
    - Information that may jeopardize facility security.
    - Formal or official communications that merit a printed or electronic document because of their importance.

- Mixing Personal and Work Accounts and Devices
  Email accounts or devices that contain both work and personal emails are subject to discovery through GRAMA requests and are therefore highly discouraged. Privacy of personal communications cannot be ensured under such circumstances. Employees should not have their work email forwarded to their personal account or personal emails forward to their work email account.

- Enforcement of Appropriate use of Electronic Mail System
    - River Heights City reserves the right and responsibility to enforce appropriate use of its electronic mail system.
    - The City's IT department has universal access rights to all email so they can monitor and ensure system security.
    - The mayor or designee will review alleged violations of the email appropriate use policy on a case-by-case basis. Violations of the policy that are not promptly remedied may result in termination of internet and email services for the person at fault.

RECORDS RETENTION AND DETENTION

The purpose of the e-mail retention policy is to ensure that e-mail and electronic documents are maintained in accordance with the Utah Government Records Access and Management Act (GRAMA).

To ensure that all official and important electronic information is not lost because of improper deletion or management of e-mail correspondence, official city emails are saved and fully archived through an offsite archiving system administered by the city's IT department. This system is independent of local emails that can be deleted or filed. These archives can be accessed by city approved officials at any time but are not accessible to employees in general.

ASSIGNMENT OF EMAILS

- City emails are assigned by position/title to employees, mayor, and council members. Upon employment/taking office, city personnel will take over the email account of the person who previously held their position.

- Passwords will be changed at the time an email changes from one person to the next.
- Email addresses are the property of River Heights City.
- Included with email, the user will have access to Google Docs, Drive and Calendar.