LYNNWOOD
WASHINGTON

Electronic Messages, Email and Electronic Records Retention Policy		Policy Number: EXE-004-2021
Policy Effective Date:	8/25/2021	**Supersedes:** N/A
Mayor: Nicola Smith	**Information Technology Director:** Will Cena	**City Clerk:** Karen Fitzthum

Applicability - This policy/procedure applies to all electronic records, email, and electronic messages, sent, or received by a City employee or elected official for City business.

Purpose – The City of Lynnwood is required to manage electronic records, email, and electronic messages as a public record, subject to preservation and destruction requirements under RCW 40.14 and RCW 42.56. This policy establishes guidelines and procedures to ensure that the City maintains compliance with laws governing records retention and email disclosure requirements. This policy is managed by the City Clerk and the Information Technology Department.

The City recognizes access to judiciary electronic records are governed under General Court Rule 31 and 31.1. Judicial Branch records are not subject to the Public Records Act.

Policy

The City owns all electronic records, email, and electronic messages: created, sent, received, or stored (1) for the conduct of City business; (2) stored on City-owned devices or systems; or (3) with City resources. All electronic records, email, and electronic messages owned by the City may be reviewed, audited, intercepted, accessed, and disclosed without employee authorization. No employee has any privacy interest in any electronic record, email, or electronic messages owned by the City.

General Court Rule 31.1 (k)(5) states “A person or entity entrusted by a judicial officer, court, or judicial agency with the storage and maintenance of its public records, whether part of a judicial agency or a third party, is not a judicial agency. Such person or agency may not respond to a request for access to administrative records, absent express written authority from the court or judicial agency or separate authority in court rule to grant access to the documents.”

References

City of Lynnwood Administrative Policy HR–755–2009 Technology Recourse use Policy

Definitions

Electronic Records: Any record, including documents, recordings, and/or data created or used by the City for the conduct of business. Examples include, but are not limited to correspondence, recordings of meetings by minutes, visual recordings, sound recordings, and recording of chat exchanges within and between staff and other users.

Email: records within the standard email program Outlook and any successor program used for the City.

Electronic Messaging: Any record sent or received by the City using instant messaging, chat groups, or similar functions in messaging systems.

Transitory records or messages: Records that do not contain evidence of actions, decisions, approvals, or transactions of City business and are not subject to retention by the state.

1. Email

1.1. Every City of Lynnwood official and employee who conducts City business using City-provided email service is individually responsible for complying with the City's guidelines.

1.2. Emails are records that may contain evidence of actions, decisions, approvals, or transactions of City business and are subject to retention requirements. Each employee is responsible for determining which retention period applies to the content of each email.

1.3. Storing emails outside of the City's email servers is prohibited unless it is in conjunction with a pending Public Records Act request or a long-term storage application approved by the IT Director and City Clerk. Examples of prohibited storage include, the use of PST files, saving individual emails to a folder location, and storing printed copies. These files cannot be located properly by IT when needed.

1.4. Knowingly deleting emails responsive to a pending Public Records Act request is prohibited, even if the retention rules would otherwise allow such deletions.

1.5. The City is required to keep one primary copy of the record. For emails exchanged between departments of the City, the sender is responsible for determining the archive value of the email and retaining the primary copy when required.

1.6. Emails received from an external source may be considered a primary copy depending on the content. The receiver is responsible for determining the archive value, if any, of the email received. Replies are considered a primary copy.

1.7. Standard Retention - Emails received must be assessed for retention value within 90 days. Each employee has the option of moving the email into a retention folder or deleting it. Emails not deleted or moved to a retention folder will be automatically deleted after 90 days (permanent retention exceptions noted below). Retained emails may be moved to one of the following retention folders:

Three-year Retention – Emails with retention requirements up to 3 years from the date received must be archived in the 3-year folder. Individual emails will be automatically deleted after the 3-year retention period. Subfolders used within this folder will inherit the 3-year retention policy.

Ten-year Retention - Emails with retention requirements of 3 to 10 years from the date received must be archived in the 10-year folder. Individual emails will be automatically deleted after the 10-year retention period. Subfolders used within this folder will inherit the 10-year retention policy.

Sent Folder Retention – Email sent must be assessed for retention value. Emails not deleted or moved will automatically delete 3 years from the day it was sent

(permanent retention exceptions noted below). Subfolders used within this folder will inherit the 3-year retention period.

Permanent Retention – Internal and external communications to, from, or on behalf of the City's governing bodies, elected official(s)/executive management, and advisory bodies will be permanently archived. City Public Records Officer will determine the person(s) who belong to this category. Information Technology will advise those affected by the automatic permanence of their email. These emails have no delete date.

The judicial branch of the city, under the direction of the Presiding Judge, shall be responsible to ensure that emails sent by judicial branch city employees are retained by the court for the appropriate retention period set forth in this policy. The manner in which judicial branch emails are stored are at the discretion of the Presiding Judge.

2. ELECTRONIC MESSAGES (TEXT MESSAGES/INSTANT MESSAGING)

2.1. **Authorized Use -** Text messages may only be used for transitory communications. Sensitive information must not be sent by text message, including social security numbers, credit card numbers, and passwords.

2.2. Employees may use Microsoft Teams for instant messaging and in place of text messages. Website integrated chat applications may also be utilized, provided they are searchable for Public Record Act requests and approved by the IT Director.

2.3. At the request of the City employees are required to provide to the City any text messages concerning City business, including those on personal devices or accounts.

2.4. **Retention –** Delete transitory text messages from the device as soon as the message has served its purpose. In no event shall employees store text messages concerning City business on their device longer than one year.

3. ELECTRONIC RECORDS

3.1. **Authorized Use -** An electronic record is typically created by the original author or a subsequent author who edits the original record. This editing may create a new version of the record. The creator, or "owner," of electronic records is considered the custodian.

3.2. An electronic record must be stored on City storage device, as determined by the Information Technology Director. Employees should not save electronic records on local computer drives, such as the C: drive or desktop. Limit the use of temporary storage before transferring the electronic record to a searchable shared drive.

3.3. City managed Microsoft SharePoint and OneDrive sites are the approved cloud storage solution. These two tools may be used to share file outside the City. Records may **NOT** be stored on portable media, personal devices, or personal "Cloud" storage (including but not limited to Dropbox, Google Drive, iCloud). To the extent a different solution is necessary to facilitate a file transfer, contact the IT Department for an approved solution.

3.4. At the request of the City, or Presiding Judge for judicial branch, employees must turn over any electronic records concerning City business, including those on personal devices or accounts.

3.5. **Retention -** It is the employee's responsibility to store records in an approved storage format for the required retention period. The retention period is established in the City and State's records retention schedules. There may be additional holds such as when there is an Public Records Request or Litigation Hold Notice is in place.

3.6. When an employee leaves their position, the employee's manager is responsible for designating a new custodian for their records. The manager ensures that the records are identified and, when appropriate, transferred to another location before deleting the prior employee's accounts.

4. TRAINING

4.1. Upon policy adoption, all City employees with a network account will be required to attend training on their responsibilities and acknowledge the policy in writing. The training will cover how to comply with the policy.

4.2. Every new City employee responsible for city records will receive training on this policy within one month of his/her/their hire date. The City Clerk, in coordination with Information Technology Director, will develop training and maintain the records of training attendance.

4.3. The judicial branch is responsible to train judicial branch city employees on the storage and retention of court case and administrative records.

5. AUDITING

5.1. The City or Presiding Judge for judicial branch employees may perform reviews to make sure all employees are complying with this policy.

5.2. Failure to comply with this policy may lead to corrective actions up to and including termination of employment.

5.3. Department directors, managers, and supervisors are responsible for the enforcement of this policy.

6. TOOLS AND TECHNOLOGY

6.1. Any new records tools or technologies must be reviewed and approved by the Information Technology Director, after consulting with Public Records Officer, before purchase, use, and implementation in accordance with LMC 2.92.100 (F).