


# Electronic Mail and Internet Access Policy

---

	<b>Louisiana Department of Health (LDH)</b>	
	<b>Policy Number</b>	66.3
	<b>Content</b>	Establish LDH rules for the use of electronic mail and internet access systems provided by the Division of Administration, Office of Technology Services (DOA/OTS)
	<b>Effective Date</b>	February 18, 2020
	<b>Inquiries to</b>	Office of Management and Finance Division of Human Resources, Training and Staff Development P. O. Box 4818 Baton Rouge, Louisiana 70821-4818 (225) 342-6477 FAX (225)342-6892

LDH is committed to fostering, cultivating and preserving a culture of equity, diversity and inclusion. Our human capital is the most valuable asset we have. The collective sum of the individual differences, life experiences, knowledge, inventiveness, innovation, self-expression, unique capabilities and talent that our employees invest in their work represents a significant part of not only our culture, but our Department's reputation and achievement as well.

If there is a discrepancy between an LDH Policy and a Program Office or facility policy, the LDH policy shall govern/override/supersede the conflicting section within the Program Office or facility policy.

## I. POLICY STATEMENT

In order to empower its employees to perform their best work, LDH uses the statewide email and internet access systems provided by the Division of Administration/Office of Technology Services (DOA/OTS) to enable employees to efficiently share information necessary to conduct Departmental business and access information needed for the conduct of LDH's programmatic and administrative business. Use of these systems shall not interfere with employees' assigned duties and shall be subject to the provisions contained in this policy.

This policy also establishes LDH rules for the use of electronic mail that pertains to Federal Tax Information (FTI). Please see Section IV.L of this policy.

LDH employees do not have a right to, or expectation of, privacy while using any government-issued equipment or systems at any time.

## **II. APPLICABILITY**

This policy is applicable to all employees of LDH.

## **III. RESPONSIBILITIES**

Appointing authorities and their designees are responsible for determining their subordinate employees' need for access to state email and/or internet access systems.

Supervisors are responsible for determining whether email use and/or internet use by employees under their supervision is interfering with the employees' productivity and shall take corrective action when necessary.

## **IV. ELECTRONIC MAIL POLICY PROVISIONS**

- A. The primary purpose of state email is to assist employees in fulfilling their duties and responsibilities. Any other use is prohibited.
- B. Personally Identifiable Information (PII) and Protected Health Information (PHI) shall not be sent outside the state email system unless encrypted using DOA/OTS approved software. (For example, do not email PII or PHI from your state email account to your personal email account.) If the employee must send PII or PHI outside of the state email system (as directed or approved by the appointing authority or their designee) and does not know how to do so, they should submit a service request to the DOA/OTS Service Desk for assistance.
- C. Employees must not send, forward or request that confidential or sensitive information be sent to them through non-LDH email accounts such as Gmail, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
- D. Employees shall use the Louisiana Statewide Email Web Access for accessing state email from outside the state network.
- E. Users should be aware that any email sent from their state email account is not private and is subject to viewing. All state email is retained at the Division of Administration and may be reviewed or made public for (but not limited to) the following reasons:

1. Public record request
  2. Judicial order and/or subpoena
  3. Suspected system misuse
  4. Information security breach
- F. The following activities are strictly prohibited:
1. Using state email to create any offensive or disruptive messages, such as use of obscene language, harassment or violation of any federal, state or LDH policy or regulation.
  2. Using state email to conduct personal business.
  3. Using state email for political campaigning or lobbying.
  4. Violating copyright laws by distributing protected works through the state email system without appropriate authorization.
  5. Posing as anyone other than oneself when sending state email, except when authorized to do so by the appropriate email account user.
  6. Using email software other than the system provided by DOA/OTS to conduct state business.
  7. Using state email to solicit for personal commercial ventures or personal gain.
  8. Sending or forwarding attachments through state email with the intent to distribute computer viruses.
- G. State email users shall not use state email to subscribe to mail lists or list servers that are not related to official departmental business or professional enhancement in support of the agency's mission.
- H. Any messages to be sent to all state email users in LDH must have the approval of the Bureau of Media and Communications before being sent.
- I. Attachments to state emails shall not exceed thirty (30) megabytes. Larger files shall be transferred by other methods such as using secure FTP or shall be zipped as smaller files using approved software.

- J. Default background shall be used for state email to provide a professional look and readable content. Custom backgrounds shall not be used for state email.
- K. The employee's state email signature shall not include personal greetings, images or URL's that are not LDH business-related.
- L. Federal Tax Information (FTI)
  - 1. FTI is any Federal Tax Information or data received through the Federal Data Services Hub via the IRS, CMS, or any other entity acting on behalf of the IRS, and which is accessed through the LDH Medicaid FTI Vault application. This information may be in whole or in part in any form (electronic, written, spoken, photocopied or screen printed, etc.)
  - 2. FTI is protected by law to safeguard sensitive personal and financial information about taxpayers.
  - 3. Protecting FTI sent or received via email and/or fax:
    - a. The following activities are prohibited with LDH: transmitting FTI via email and/or fax.
    - b. It is prohibited to email FTI either as an email or as an attachment to an email. Do not open any email that contains FTI but report the occurrence to your supervisor for logging and tracking until the deletion of the email. If FTI is inadvertently emailed, report the occurrence to your supervisor for logging and tracking until the disposition of the email. The supervisor will contact unintended recipients to request and confirm destruction of the information.
    - c. Faxing FTI is prohibited. If FTI is inadvertently faxed, report the occurrence to your supervisor for logging and tracking until the disposition of the fax. The supervisor will contact unintended recipients to request and confirm destruction of the information.
  - 4. **Tax return**/information received directly from the taxpayer or obtained from public information files is not considered protected FTI that is subject to the safeguarding requirements. If the taxpayer or third party subsequently provides returns, return information or other Personally Identifiable Information (PII) independently, the information is not FTI as long as the IRS source information is replaced in FTI application with the new provided or obtained tax information.

## V. INTERNET ACCESS POLICY PROVISIONS

- A. The primary purpose of state internet access is to assist employees in fulfilling their duties and responsibilities. **Brief** and **occasional** use of state internet access for other reasons is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to LDH or otherwise violate this policy. Use is defined as “excessive” if it interferes with normal job functions, responsiveness or the ability to perform daily job activities.
- B. This policy does not apply to the LDH Intranet access which is granted to all LDH employees with appropriate computer equipment and software.
- C. Use of state internet access for any purpose other than legitimate LDH business or LDH research is strongly discouraged.
- D. Internet material must be scanned at the time of download using currently updated anti-virus software (This function is done automatically and does not require action by the user).
- E. Any employee who suspects that their computer has been hacked should immediately report the problem to DOA/OTS.

## VI. TRAINING

Current LDH employees shall complete a training course on this policy annually by accessing and completing the course in the learning management system provided by the Division of Administration in the Louisiana Employees Online (LEO) system. New employees shall complete this course within 90 days of the date of hire.

## VII. VIOLATIONS

Violations of this policy may result in corrective action or disciplinary action. Corrective action includes Improvement Letters (Civil Service Rule 12.9). Disciplinary actions are Suspension without Pay, Reduction in Pay, Involuntary Demotion and Dismissal (Civil Service Rule 12.3). Any corrective or disciplinary action taken is at the sole discretion of the Appointing Authority.

## VIII. REFERENCES

Copyright Act of 1976

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

## IX. REVISION HISTORY

Date	Revision
March 31, 2000	Policy created
June 29, 2004	Policy revised
May 1, 2008	Policy revised
July 27, 2011	Policy revised
November 7, 2013	Policy revised
February 18, 2020	Policy revised
June 7, 2023	Policy updated (Section IV.L added – page 4)
October 16, 2024	Policy reviewed