FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Electronic Mail (Email) Access and Use Procedures

Related Policy: FDJJ – 1220

I. DEFINITIONS

Confidential Information – Information made confidential by state or federal law and thus is not subject to public inspection. This information may only be released to those entities and persons listed in statute. Examples of confidential information includes, but is not limited to, Driver's License Numbers, Social Security Numbers, employee health information, employment and drug screening results, and any information that would identify a youth under the Department's jurisdiction such as names, charges, case numbers, location, etc., under Chapter 119, F.S.

Email – Electronic mail messages sent to users on the local or wide area network or to anyone on the Internet who has an email account.

Encryption – The reversible process of scrambling readable text into unreadable (or cipher) text so unauthorized people are not able to read the message content.

Public Records – Public records are any materials made or received by a public agency as part of its official business, as per Section 119.011(12), F.S.

Tagline – Extraneous information, such as slogans, quotes, sayings, catchphrases, symbols, graphics, images, pictures, animations, etc., added to an email or email signature block.

II. STANDARDS/PROCEDURES

A. Acceptable Uses of Email:

1. Although the Department of Juvenile Justice does not prohibit all personal use of email, a common sense approach should be applied. The agency shall have sole discretion to determine whether a use is personal or business.

2. Associates are permitted limited personal use of information resources if the use does not result in a loss of associate productivity, interfere with official duties or business, and involves minimal additional expense to the government.

3. Acceptable limited personal use of email is where the communication is brief, does not interfere with the normal performance of a worker's duties, does not consume significant amounts of state information technology resources, does not subject the Department to any additional cost, does not involve an employee's personal business enterprise, is not otherwise prohibited by Florida law or Department policy, and is consistent with the requirements contained in this policy and other policies related to the employee's responsibilities and duties.

4. Department sender email signature blocks are limited to the following components:
   a. Closing phrase (Sincerely, Thanks, Best, Respectfully, Best Regards, Yours Truly, etc.)
   b. Name
   c. Professional designations
   d. Department name (DJJ, Department of Juvenile Justice, Florida Department of Juvenile Justice, etc.)
   e. Department Position/Title
   f. Work phone numbers (office, cell, fax, etc.)
   g. Postal mail address
   h. Email address
5. Department sender email signature blocks shall not include taglines unless they list the Department's Mission, Values, Vision, Roadmap Statement, and/or are approved statements related to Departmental initiatives, business operations, or juvenile justice information. Requests to include a tagline to an employee's email signature block shall be submitted to the Office of Communications for approval, if appropriate.
6. Email containing confidential information shall carry a notice, warning the recipient of the confidential nature of the information and the applicable limits on its use and subsequent disclosure.

   Sample Disclaimer:

   Information regarding children is confidential pursuant to section 985.04, Florida Statutes. This information is provided to you solely for the purpose for which it was requested. Any further dissemination and/or exposure is prohibited and could result in disciplinary action up to and including dismissal, civil fines or tort action, and/or criminal penalties under applicable state and federal regulations and laws.

B. Prohibited Uses of Email include:

1. Non-state sponsored solicitations, including but not limited to such things as advertising the sale of property or other commercial activities;
2. Auto-forwarding Department email messages to personal/privately owned email accounts or personally-owned devices;
3. Sending copies of documents in violation of copyright laws or licensing agreements;
4. Sending messages prohibited or restricted by government security laws or regulations or any other communication, which may adversely affect the Department's ability to carry out its mission;
5. Sending messages which may reflect unfavorably on the Department, or which may be perceived as representing the Department's official position on any matter when authority to disseminate such information has not been expressly granted in writing;

6. Sending confidential or proprietary information or data to persons not authorized to receive it, either within or outside DJJ;

7. Sending messages or requesting information or material that is fraudulent, harassing, obscene, offensive, discriminatory, lewd, sexually suggestive, sexually explicit, pornographic, intimidating, defamatory, derogatory, violent, or which contains profanity or vulgarity, regardless of intent:

   Messages which are considered offensive include, but are not limited to, messages containing jokes, slurs, epithets, pictures, caricatures, or other material demonstrating animosity, hatred, disdain or contempt for a person or group of people because of race, color, age, national origin, gender, religious beliefs, marital status, disability, sexual orientation or any other classification protected by law;

8. Sending material promoting political positions or actions;

9. Sending malware;

10. Sending SPAM;

11. Sending "Chain" letters; and

12. Forging/Spoofing email headers.

C. Requests for Access to Content of Email:

1. Any requests for access to the contents of email in order to respond to a legal process, such as subpoenas and public records law requests, or for purposes involving litigation, investigation or claim, must be immediately be brought to the attention of the Office of General Counsel.

D. Establishment of Email Accounts:

1. All email accounts must be established, terminated, or transferred via a Network User Account Request or a Network User Account Deletion form, as per FDJJ 1205.50.

E. Employee Rights to Personal Email Privacy:

1. Department employees have no right of personal privacy in any material created, stored in, received, or sent over the Department's email system.

2. Managers/Supervisors shall have access, upon request, to the email of employees under their direct supervision.

3. The Department reserves and may exercise the right, at any time and without prior notice or permission, to intercept, monitor, access, search, retrieve, record, copy, inspect, review, block, delete, and/or disclose any material created, stored in, received or sent over the Department's email system for the purpose of protecting the system from unauthorized or improper use or criminal activity.

F. Confidential Information:

1. Email between or amongst employees of the Department or those acting on behalf of the Department may include confidential information; and email to law enforcement, judicial offices and schools as permitted by law, may contain confidential information based on the following guidelines: Confidential information should never be in the subject line of any Email message. Only the minimum amount of information necessary to perform official duties of the Department should be included in an email.

2. It is the responsibility of the individual's supervisor to provide direction on the routine protection of confidential information in accordance with their specific job duties and functions.

G. Email Encryption Criteria:

1. Employees shall ensure outbound messages are encrypted by typing the word "Confidential" or "Encrypt" anywhere in the subject line of messages containing the following exemption criteria as outlined in Florida Statute:

   a. U.S. Social Security Numbers: 119.071(4)(a), F.S. and 119.071(5)(a)5, F.S.
   b. U.S. Driver's Licenses Numbers/Motor Vehicle Records: 119.712(2)(b), F.S.
   c. Banking and Credit Card Information: 119.071(5)(b), F.S.
   d. Personally Identifiable Youth Information (currently or formerly in DJJ care): 985.0(7)(a), F.S.
   e. Personally Identifiable Information of parents/guardians of youth in DJJ care or victims: 985.04(7)(a), F.S. and 119.071(2)(h)-(j), F.S.
   f. Personally Identifiable Information of child abuse or sex offense victims: 119.071(2)(h)-(j), F.S. Residential information of the DJJ's Direct Care Staff (119.071(4)(d)1.i., F.S.)
   g. Medical/mental health information of past or present DJJ employees (119.071(4)(b)1, F.S.).

Employees shall ask for their supervisor's assistance and direction if they have any questions regarding maintaining or emailing confidential information.

NOTE: Encrypting confidential information sent by email is required by FL Administrative Code 71A-1.

Typing the word "Encrypt" or "Confidential" in the subject line of confidential messages is an internal procedure intended for DJJ staff (and Providers, Contractors, and Vendors who use DJJ's email system) to encrypt the confidential data sent via the Department's email system.

External providers, contractors, vendors, etc. using their own email system are responsible for encrypting the confidential information sent by email.

H. Email Retention Requirements:

1. Email public records, as defined in this policy, must be retained according to approved retention schedules for State Government Agencies, which can be found at http://dos.myflorida.com/library-archives/records-management.

2. It is the responsibility of each Department employee to ensure email and other public records in their custody are maintained for the required retention period(s). Although the Department routinely backs up its servers, each back-up is maintained for brief periods only for disaster recovery purposes and therefore cannot be regarded as a tool for meeting public records retention requirements.

3. Retention periods for emails are determined by the content, nature and purpose of records, and are established based on their legal, fiscal, administrative and historical values, regardless of their form. Therefore, there is no single retention schedule that would apply across the board to all emails.

4. Email, like other records, irrespective of form, can have a variety of purposes and relate to a variety of program functions and activities. The retention period for any particular email message will generally be the same as the retention period for records in any other format documenting the same program function or activity.

I. Penalties for Violation:

1. Violation of any provision of this policy is cause for disciplinary action up to and including dismissal, civil fines or tort action, and/or criminal penalties under applicable state and federal regulations and laws.

III. RESPONSIBILITY AND DUTIES

A. Department of Juvenile Justice Employees:

1. Employees shall be held responsible for security and integrity, to the degree that his or her job requires the use of the email system. Fulfillment of these responsibilities shall be mandatory, and violation of security requirements or other provisions of this policy may be cause for disciplinary action.

2. Employees should not open email messages from unknown sources to avoid viruses. If an authorized user/employee receives an email containing a virus, they are to immediately contact their local Bureau of Information Technology representative.

3. Upon request, all employees shall give their immediate manager/supervisor "reviewer" authority over their electronic mail inbox.

4. Submit requests to DJJ Office of Communications for approval of a tagline.

B. Managers/Supervisors:

1. Managers/Supervisors shall ensure those employees under their direct supervision have been provided adequate direction regarding the protection of confidential information, as per FDJJ 1215, *Information Security Awareness Training Policy.*

2. Managers/Supervisors shall provide direction to those employees under their direct supervision on the protection of confidential information in accordance with their specific job duties and functions.

3. Manager/Supervisors shall have access, upon request, to the email of employees under their direct supervision. If needed, contact your local Bureau of Information Technology representative for assistance.

4. In the event a Manager/Supervisor did not gain access to an employee's email account, and the employee is out of the office for an extended amount of time (e.g., example medical or administrative leave), the employees' direct Manager/Supervisor may request to access their email by completing and submitting the "Request to Access Electronic Mail of Others" (Attachment 1).

C. Office of Communications:

1. Review requests to add taglines to an employee's email signature block and communicate approval/disapproval to the requester.

IV. ATTACHMENTS

ATTACHMENT 1 - REQUEST TO ACCESS ELECTRONIC MAIL OF OTHERS