I. POLICY:

Employees shall use the Department of Juvenile Justice electronic mail (e-mail) to enhance productivity in support of the Department’s mission and goals. Each e-mail user shall utilize these resources efficiently and productively, safeguard them from unauthorized access and misuse, and refrain from using them inappropriately and/or for prohibited purposes.

II. DEFINITIONS:

E-Mail: A method of communication that consists of the sending and receiving of electronic messages, information, and files through the internal networks of the Department and/or the internet.

IT Director: Director of the Office of Technology and Information Services.

III. PROCEDURES:

A. Office 365 is the only authorized email service for the Department.

B. DJJ may provide authorized users access to the DJJ’s e-mail system. Access to the e-mail system is a privilege, not a right.

C. As part of standard practice to prevent loss of data, DJJ’s e-mail system and systems involved in the transmission and storage of e-mail messages will be “backed up” on a routine basis. This process results in copying data, including the contents of e-mail messages, onto storage media that may be retained for periods of time in locations unknown to the sender or recipient of a message.

D. The Office of Technology and Information Services (OTIS) may be required to monitor the network and e-mail system and/or troubleshoot problems. OTIS
staff may view the contents of e-mail messages during the performance of their duties. Employees have no expectation of privacy with respect to their email messages or usage.

E. E-mail accounts shall be password protected. Passwords are considered confidential and will be handled according to the policy DJJ 6.8, IT Security.

F. E-mail and other electronic files may be accessible through the discovery process in the event of litigation.

G. Staff will archive emails as necessary when the mailbox is full and will retain all emails in accordance with the Record Retention Schedule (see DJJ 5.1, Records Management).

H. In order to standardize the appearance of email messages and save network space, users may not insert unauthorized graphics or personalized messages, and may not use stationary (e.g., borders, colors, etc.). Email graphics will be limited to only approved logos, (Attachments A and B).

I. All DJJ email users are required to include a signature line in DJJ emails.

1. A DJJ email user’s signature line will contain the following information:
   a) Name;
   b) Title; and
   c) Office Phone Number, if applicable.

2. A DJJ email user’s signature line may include the following information:
   a) Business address;
   b) DJJ-issued mobile communications device number;
   c) FAX number; or
   d) A small graphic, limited to DJJ Seal or GA state flag, not to exceed 1 inch in diameter.

J. All e-mail sent to persons outside the Department will be treated as formal correspondence. As such, all users of DJJ’s e-mail system will exercise care to ensure this correspondence is prepared in a professional manner.

K. DJJ e-mail system users will exercise care when transmitting sensitive or confidential information because e-mail messages can be re-transmitted. In
doing so, users will adhere to all policies regarding the distribution of sensitive/confidential information.

L. No DJJ official e-mail or its attachments may be forwarded or downloaded to any personal e-mail account and/or personal electronic device.

M. An employee using the DJJ’s email system has no right to or expectation of privacy. To the maximum extent permissible by law, DJJ may monitor, investigate, retrieve and read any communication or data composed, transmitted or received through DJJ’s email system without notice to an employee. This includes any information stored on the DJJ’s servers or property. This includes all system configurations and all files on those systems.

N. If an employee is aware of any breach in information security, it will be handled in accordance with DJJ 6.2, Network Access and 6.8, IT Security.

O. DJJ will handle security breaches according to procedures established by the Georgia Technology Authority and the IT Director.

I. LOCAL OPERATING PROCEDURES REQUIRED: NO