

| | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| GEORGIA DEPARTMENT OF JUVENILE JUSTICE | Transmittal # 17-14 | Policy # 6.2 |
| Applicability <input checked="" type="checkbox"/> All DJJ Staff <input type="checkbox"/> Administration <input type="checkbox"/> Community Services <input type="checkbox"/> Secure Facilities (RYDCs and YDCs) | Related Standards & References: Georgia Technology Authority Policies, Standards and Guidelines ACA Standards: 4-JCF-6F-01, 3-JDF-1E-07, 08 | |
| Chapter 6: INFORMATION TECHNOLOGY | Effective Date:12/15/17 | |
| Subject: NETWORK ACCESS | Scheduled Review Date:12/15/18 | |
| Attachments: | Replaces: 10/20/14 | |
| None | Administrative Services Division | |
| APPROVED: | | |
|  | | |
| <hr/> Avery D. Niles , Commissioner | | |

I. POLICY:

Department of Juvenile Justice information technology (IT) resources shall be used to enhance employee productivity in support of the Department’s mission and goals. Each user of IT resources will 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:

Approving Manager: An individual’s supervisor. The Approving Manager may designate a subordinate manager to act on his or her behalf to perform this function using the Approving Manager’s Designee Form. For the purpose of this policy, the Regional Health Services/Behavioral Health Services Administrator or Regional/Area Principal will be the approving manager for staff in their respective subject areas.

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

Information Technology Resources: Desktop, laptop, and handheld computers and tablets, jump/flash drives used on Department computers, printers, scanners, data networks and servers, internet, e-mail, numerous applications including but not limited, to mobile platforms and software programs, cellular telephones, Guard Plus, DJJ agency website, CCTV, wireless, electronic and video communications devices.

III. PROCEDURES:

- A. Access to DJJ’s information technology (IT) resources is a privilege, not a right. The Office of Information and Technology Services (OTIS) may deny or revoke access at any time without notice.
- B. Access to all networked resources, including all applications and services provided through them, must be approved by the IT Director or designee.

| Chapter | Subject | Policy # | Page |
|------------------------|----------------|----------|--------|
| INFORMATION TECHNOLOGY | NETWORK ACCESS | 6.2 | 2 of 3 |

1. All users\persons accessing DJJ’s network must electronically sign the Information Security Agreement acknowledging appropriate use of the DJJ’s IT resources before a user\person is allowed to access the DJJ’s network. The user’s supervisor is responsible for ensuring that the user completes the Information Security Agreement prior to requesting network access for that user. Thereafter, the Information Security Agreement will be electronically reviewed and signed at the discretion of the IT Director or designee. (See DJJ 6.8, IT Security.)
 2. To gain network access, the Network Access/Removal/Transfer Form on the DJJ Intranet will be submitted for the individual requesting access by the end of the new employee’s on-the-job training period. For employees, the form must be approved by the Approving Manager. The Office of Technology and Information Systems (OTIS) will notify the Approving Manager of status.
 3. When an employee transfers within the DJJ (i.e., to another facility/program, another job title, etc.), the Network Access/Removal/Transfer Form must be submitted prior to executing the transfer. The Employee’s responsible manager must approve the transfer. In the event a transfer is not properly executed the employee’s access shall be immediately disabled until the proper completion of the transfer paperwork.
 4. When a user is terminated or no longer needs access to the network, his/her supervisor will inform OTIS verbally and complete and submit the Network Access/Removal/Transfer Form prior to the end of the employee’s last working day. The only exception is when an employee’s removal is unplanned. Failure of a supervisor to notify OTIS of the need to remove the employee’s access both verbally and via the Network Access/Removal/Transfer Form may result in disciplinary action.
 5. For users outside of DJJ requesting access (e.g., judges), the request and supporting documentation must be submitted to the Office of Legal Services for review and upon approval by the Commissioner or designee, network access will be granted.
- C. The Department is not responsible for the destruction, corruption or disclosure of personal material on or by its IT resources.
- D. The Department may remove, replace, or reconfigure its IT resources without notice. Connection of a device to the network can be accomplished with the approval of the IT Director or designee.
1. Georgia Technical Authority (GTA) or higher agencies shall not disallow connection or control of the department’s networks by default without specific denial, disapproval, or ruling with specific justification.

| Chapter | Subject | Policy # | Page |
|------------------------|----------------|----------|--------|
| INFORMATION TECHNOLOGY | NETWORK ACCESS | 6.2 | 3 of 3 |

2. In the event GTA or a higher agency determines that an IT resource should not be connected to the Department's network that device can remain connected while the policy is being verified or challenged.
 3. The Department shall ask for approval only where there is a clear conflict or specific issue with the policies.
- E. No individual may utilize any personally owned IT resource, including software, on DJJ computers and/or networks without the approval of the IT Director or designee.
- F. DJJ may provide authorized users access to the internet and other outside networks. (For youth in custody see DJJ 13.13, Youth's Internet Use and Safety.)
1. Outside networks may include offensive/objectionable materials. DJJ will not be responsible for the nature or content of any outside networks encountered by users.
 2. Limited personal use of the internet will be permissible where it involves no additional expense to DJJ and is done in accordance with the Information Security Agreement.
 3. Employees must keep personal use of the internet to a reasonable duration and during personal time (e.g., before/after work hours, meal periods, breaks, etc.). Personal use of the internet must never interfere with DJJ's mission. (See also DJJ 6.6, Social Media.)

IV. LOCAL OPERATING PROCEDURES REQUIRED: NO