Chapter: Conditions of Employment **Effective Date:** 12/1/11
Title: Use of Information Technology Resources **Page:** 1 of 6
New

ACA Standard(s): N/A
Reference(s): 1 TAC §202.25, GAP.05.07

(a) **Policy.**

Texas Juvenile Justice Department (TJJD) employees, and non-TJJD employees who have access to TJJD information technology resources, shall use professional practices in using information technology resources. All agency information technology resources are the property of TJJD and the State of Texas and are provided for the conduct of state business. TJJD has established rules for the use of information technology resources.

(b) **Definitions.**

(1) **Information Technology Resources –** include, but are not limited to, information technology systems, information technology hardware (desktop and portable computers, printers, pagers, phones, cell phones, personal digital assistants, radios, multi-function printer/copiers and fax machines), information technology software (commercially packaged software and internally developed software), information systems, and communication systems.

(2) **Non-TJJD Employees** – include, but are not limited to, any of the following who have access to TJJD information technology resources: contractors, employees of contractors assigned to TJJD, and volunteers/interns. These persons shall adhere to this policy as stated in their agreements and contracts.

(3) **Non-Work Time –** off-duty hours such as before or after a workday (subject to local office hours), meal periods, or authorized breaks.

(4) **Minimal Additional Expense –** the cost which results when small amounts of electricity, ink, toner, paper, or time are used. The cost resulting from brief personal telephone calls, personal e-mail, or brief Internet sessions are also examples of minimal additional expense. The cost involved in downloading large files (such as motion picture video or the contents of an entire compact disc), or forwarding holiday greetings or chain letters throughout the network is not minimal additional expense.

(5) **Personal Use –** non-commercial use of information technology resources for purposes other than accomplishing official or otherwise authorized activity. Examples of authorized personal use would include communicating with a volunteer charity organization or scheduling a medical appointment.

(c) **General Provisions.**

(1) State property is intended for use in conducting state business. However, personal use of certain information technology resources is not considered misuse of state property within the limitations provided in this policy. Personal use may be permitted as long as such use:

(A) involves minimal additional expense to the state, unless otherwise restricted;

(B) does not impede the agency's functions by interfering with performance of official TJJD duties, operations, and normal work activities;

(C) is not for private commercial purposes;

(D) is not political in nature;

(E) is not inappropriate;

(F) is performed on the employee's or non-TJJD employee's non-work time;

(G) does not violate standards of ethical conduct for employees or non-TJJD employees; and

(H) does not damage the reputation or credibility of the agency.

(2) Use of information technology resources for personal use other than outlined above, or for any business other than that specified in state security rules and procedures and authorized by TJJD, is grounds for disciplinary action up to and including termination.

(3) A pattern of improper use shall not be considered accidental and is grounds for disciplinary action up to and including termination.

(4) All inappropriate use or misuse of information technology resources shall be reported to the TJJD information security officer in Central Office.

(5) Employees and non-TJJD employees are responsible for protecting agency information residing on personally owned information technology resources.

(6) Employees shall sign the TJJD Information Security and Non-Disclosure Agreement form, HR-016, during new employee orientation. Non-TJJD employees who have access to TJJD information technology resources shall sign the HR-016 form prior to commencing their assignments.

(7) Employees shall receive information security basics during new employee orientation and annually thereafter. Non-TJJD employees who have access to TJJD information technology resources must receive annual training on information security basics.

(8) The supervisor or appropriate logon authority shall annually review the access(es) that employees and non-TJJD employees have to TJJD information technology resources and report all changes to the Information Resources Division (IRD).

(9) If an employee is experiencing difficulty with an assigned cell phone, pager, mobile computing device, or radio, the employee must contact the local site network specialist to correct the issue. Employees should not attempt to correct the problem without proper assistance.

(10) In accordance with PRS.11.01, employees separating from employment must return state-issued information technology resources and accessories.

(11) IRD may monitor any TJJD information technology resource to ensure security and appropriate use of state property and state time without notice of times, locations, or duration.

(d) **Badges.**

Employees, non-TJJD employees, and other users of badges intended for access and/or identification must maintain exclusive control and use of their badge(s) and are responsible for any activity, authorized or unauthorized, resulting from the use of their badge(s).

(e) **Cellular Phones.**

(1) Agency cellular phones are for official business use. Agency cellular phones may also be used for emergency calls while on travel status, notification to family of changing schedules, and calls concerning the health or safety of employees.

(2) Requests for cellular phone service must be submitted on the Cellular Services Request form, IRD-002. The executive director or designee must approve requests for new service. Requests for changes in existing service must approved by the department director.

(3) Managers, supervisors, team leads, and end users are responsible for the prudent and efficient use of cellular phones in the field.

(4) Cell phone invoices must be reviewed monthly by department directors to ensure that staff are adhering to the terms of this policy and the service plan. Additional expenses for personal calls and/or personal overage fees for items such as text messaging, roaming, etc. shall be reimbursed by the end user. Invoice review may occur after the cell phone invoice has been processed for payment.

(5) IRD will conduct quarterly reviews of all cellular-based services to ensure that appropriate, efficient, and cost-effective services are provided to TJJD users.

(f) **Electronic Mail (E-mail).**

(1) E-mail systems must meet the retention requirements found in TAC Title 13, Chapter 6, Records Retention Schedule Rules. E-mail is subject to open record laws. Records and files are not confidential, and no privacy rights exist.

(2) All e-mail sent or received by an agency is considered a state record. All e-mail messages must be retained or disposed of according to the agency's retention schedule.

(3) E-mail is recorded and subject to monitoring.

(4) General information announcements (e.g. special event info) shall be posted to TJJD Public Folders instead of sent via bulk e-mail.

(5) Employees and non-TJJD employees are responsible for material that is received from e-mail and saved on TJJD information resources (e.g., pictures, jokes, and programs).

(6) Employees and non-TJJD employees are responsible for material that is transmitted or downloaded from the Internet through links in e-mail messages. Electronic files or programs (e.g., screensavers, programs, etc.) must not be downloaded and installed on local computers or networks unless approved by IRD.

(g) **Pagers.**

(1) Pagers must be purchased from the state contract.

(2) It is the responsibility of the appropriate manager or supervisor to approve the type and number of pagers required.

(3) Pagers are for official business only. The employee shall reimburse any expense incurred by the agency for personal pager use.

(h) **Passwords and User ID's.**

(1) Each employee and non-TJJD employee's identity and access level shall be authenticated through a unique user ID and password before access to information systems is granted.

(2) System passwords are based on the existing federal and state standards on password usage and industry best practices. For specific password requirements, see ISP.13.01.

(3) Authenticated users must maintain exclusive control and use of their user ID(s) and password(s) and are responsible for any activity, authorized or unauthorized, resulting from the use of their user ID(s) and/or password(s).

(i) **Radios and Man-Down Systems.**

(1) TJJD executive staff and facility administrative staff issue radio communications equipment to appropriate TJJD staff to continue and coordinate efforts to support and maintain a safe living and working environment for youth and staff.

(2) Each two-way radio operator/user is responsible for complying with pre-service and on-the-job training concerning proper use, as well as following operation procedures as stated in the Federal Communications Commission rules and regulations.

(3) The Youth Services Division, in collaboration with IRD, determines radio use and distribution for each campus.

(4) The director of youth services has the final decision regarding two-way radio communications operations within the agency.

(5) Each staff member who is issued a radio is responsible for verifying that the unit is working properly and promptly reporting any malfunctions or difficulties.

(6) The director of security at each campus is responsible for ensuring that only adequately trained staff members operate the radio dispatch console. IRD staff will provide training to the director of security as requested.

(7) Each staff member issued a man-down/radio unit is required to wear the unit on his/her person and maintain possession and control of the unit at all times while on duty.

(8) Each facility administrator or designee is responsible for:

(A) issuing man-down and radio units to appropriate staff;
(B) training staff in the proper use of this equipment; and
(C) reporting and securing repairs or replacement of man-down units on a priority basis.

(j) **Telephones.**

(1) Employees, non-TJJD employees, and other users of password-enabled voice mail must maintain exclusive control and use of their password(s) and are responsible for any activity, authorized or unauthorized, resulting from the use of their password(s).

(2) Voicemail passwords shall be changed at least once every 180 days. In the event of a security breach, a password change may be directed without notice.

(3) If a user experiences difficulties with a TTY device (text telephone), staff must report the issue to the local network specialist. The network specialist is responsible for providing end-user training and coordinating any needed repairs.

(4) Telephones and related devices are to be moved and configured only by the local network specialist.

(5) Employees may make long distance calls only for official agency business.

(6) Employees may make and receive personal calls that do not incur a fee for the agency as long as they do not disrupt or interfere with official state business, are kept to a minimum duration and frequency, and are not political in nature.

(7) Employees may not list their work number in classified ads, on internet sites, or in any other publication or place that is likely to generate incoming personal calls.

(k) **Web Access.**

(1) Web access is provided for legitimate state business use.

(2) Employees and non-TJJD employees must assume that all materials on the Web are copyrighted and/or patented unless specific notices indicate otherwise. Downloading and storing copyrighted material on agency information technology resources is prohibited.

(3) Bandwidth, within the agency and in providing Web access, is a shared, finite resource. Employees and non-TJJD employees shall conserve this resource and must not deliberately perform actions that waste resources or monopolize them to the exclusion of others (e.g., use of a shared workstation for personal use).

(4) Under no circumstances are employees or non-TJJD employees allowed to overload networks for personal use. This includes subscribing to list servers or websites not directly related to job responsibilities, spending extensive time on the Internet, downloading non-work files, or listening to radio broadcasts via Web access.

(5) Use of Web services (e.g., instant messaging) is for business use only.

(6) Employees and non-TJJD employees are encouraged to use the TJJD websites (Intranet and Internet) to view policies and other important agency documents.

(7) Employees and non-TJJD employees are responsible for material that is accessed or downloaded from the Web. In general, authorized materials include those from state and federal agencies, and commonly known businesses. This would not include executable files (e.g. screensavers, programs, etc.). These files must not be downloaded and installed on local computers or networks unless approved by IRD.

(8) Employees and non-TJJD employees are responsible for self-reporting and must notify their supervisor immediately if unsuitable or prohibited material is accidentally downloaded and must promptly delete the unsuitable or prohibited material.

(9) Supervisors are responsible for the prudent and efficient use of Web access including the appropriate downloading of files.

(10) Employees and non-TJJD employees must follow established agency procedures for posting information on agency websites.

(l) **Wireless Access.**

(1) IRD shall approve all wireless Local Area Network (LAN) access and equipment.

(2) No wireless access to TJJD networks, systems, or information shall be made without prior approval of IRD.

(m) **Digital Video Systems.**

Access to digital video systems (e.g., surveillance system, portable video devices) is only permitted as allowed in ISP.13.37 and ISP.13.39.

(n) **Inappropriate Use of Information Technology Resources.**

Inappropriate use of TJJD information technology resources may result in disciplinary action up to and including termination of employment. Inappropriate use or conduct includes, but is not limited to, the following:

(1) engaging in unlawful or malicious activities;

(2) misrepresenting a personal communication as a communication in the employee's or non-TJJD employee's official capacity;

(3) allowing youth access to information technology resources through an employee's or non-TJJD employee's user ID and/or password;

(4) making copies of TJJD security camera video recordings without written authorization;

(5) sending or forwarding chain letters, or “spam” (unrequested email);

(6) sending, receiving, printing, viewing, or accessing pornographic material or otherwise objectionable materials;

(7) creating a hostile work environment for other employees;

(8) using abusive, profane, racist, sexist, or otherwise objectionable language in public or private messages;

(9) any activity which causes congestion and disruption of networks and systems such as subscriptions to e-mail lists or list servers for personal use or listening to radio through Web access;

(10) defeating, or attempting to defeat, security restrictions on TJJD systems and applications;

(11) accessing another employee’s or non-TJJD employee’s e-mail or network account through use of another’s user ID and/or password;

(12) compromising confidentiality requirements or the privacy of others;

(13) engaging in commercial activities; or

(14) any political activity prohibited by agency policy.