



**DEPARTMENT OF JUVENILE JUSTICE  
AND DELINQUENCY PREVENTION**

---

**NUMBER:** DJJDP 5

**PAGES:** 6

---

**SECTION:** Information Technology

**SUBJECT:** Information Technology Resource Usage (Computer Usage)

---

**AMENDS:** DJJDP 5, IT Resource Usage

**AMENDS POLICY ISSUED:** 4/15/07

**AMENDS:** DJJDP 5, Computer Usage Directive

**AMENDS POLICY ISSUED:** 4/17/03

**APPROVED BY:** *George D. Sweat*

**DATE SIGNED:** 2/10/08

**DATE IMPLEMENTED:** 3/28/08

---

**RELATED STANDARDS:** *Information Technology Services (ITS) Policies and Standards.*

**RELATED NCAC CITATION:**

1. 28 NCAC 01A .0301, *Designated Agencies Authorized to Share Information;* and
2. 28 NCAC 01A .0302, *Information Sharing Among Agencies.*

**RELATED LEGISLATION:**

1. N.C. Gen. Stat. § 7B-3100, *Disclosure of information about juveniles;*
2. N.C. Gen. Stat. § 126-24, *Confidential information in personnel files; access to such information;*
3. N.C. Gen. Stat. § 147, Article 3D, *State Information Technology Services;*
4. N.C. Gen. Stat. § 14-454, *Accessing computers;*
5. N.C. Gen. Stat. § 14-455, *Damaging computers, computer programs; computer systems, computer networks, and resources;*
6. N.C. Gen. Stat. § 14-458, *Computer trespass; penalty; and*
7. N.C. Gen. Stat. § 114-15.1, *Department heads to report possible violations of criminal statutes involving misuse of State property to State Bureau of Investigation.*

**INDEX AS:** Information Technology Resource Usage; Business Use of Information Technology Resources; Networks; Internet Access; Computers, Business; Computers, Personal; Workstations; Desktops; Laptops; Computer Networks; Internet Access; Internet Usage; Privacy; Electronic Mail (E-mail); Data Security; Printers; E-Mail Distribution List; Help Desk; Mobile Computing; Remote Computing

---

**PURPOSE:** To ensure that all staff use Department information technology (IT) resources for Department-authorized purposes.

**POLICY STATEMENT:** IT resources are the property of the State of North Carolina and are intended for business use. All Department staff members have a responsibility to safeguard these resources by utilizing IT resources in a professional, lawful, and ethical manner, and by reporting suspected or observed computer viruses and suspected or observed unauthorized use and/or misuse of IT resources.

## I. SCOPE OF POLICY

A. This policy applies to all Department staff, which includes employees, paid and unpaid interns, cooperative education students, volunteers, temporary staff, and contractual staff.

B. This policy applies to all State-owned IT resources, in all locations of use, operated, handled, or utilized by Department staff.

C. IT resource types include software, hardware (servers, printers, laptops, desktops, wireless devices, and mobile personal computing devices), network infrastructure, e-mail, electronic data (numbers, text, images, audio, and video), the North Carolina State Network, and the Internet.

## II. ACCEPTABLE USE STANDARDS FOR IT RESOURCES

### A. General Use

1. IT resources are intended to be used for business purposes.

2. Occasional personal use of IT resources is permitted if such use does not violate any of the prohibited uses cited in this policy.

*NOTE: Examples of occasional personal use are checking status of impending severe weather conditions, floods, school closings, flight reservations, financial account balances, and webmail.*

3. Staff shall not perform activities using IT resources that:

a) Violate a federal or state law or regulation, including copyright laws;

b) Compromise public safety or public health;

c) Are deliberately and maliciously fraudulent, threatening, offensive, indecent, obscene, libelous, or slanderous;

d) Are offensive in nature and/or designed to embarrass or humiliate the State and/or the Department;

*NOTE: Reference DJJDP 13, Ethical Conduct: Code of Ethics.*

e) Interfere with the staff member's job performance;

f) Cause unnecessary traffic or decrease the performance of IT resources such as playing computer games, uploading or downloading large files, accessing streaming sites, and instant messaging; or

g) Violate any provisions, guidelines, or standards within this policy, or any other Department or State policy.

4. Only authorized persons are permitted to use IT resources. Authorized persons are:

a) Persons with an authorized computer account; or

b) Persons granted authorized temporary access and/or user rights by Technical Services, Application Development, and/or Security, depending on the IT resource.

5. Staff shall not gain or attempt to gain unauthorized access to any IT resource system including network computer accounts, data transmissions, or e-mails.
6. Staff shall not create, store, or circulate unauthorized materials using IT resources. Unauthorized materials include pornography, commercial or personal advertisements, solicitations, promotions, mass mailings, chain letters, and destructive code. Staff shall not use IT Resources to access, create, store, or circulate pornographic materials.

B. Network Infrastructure/Hardware/Software

1. No hardware, software, or network infrastructure of any kind shall be installed, downloaded, uploaded, copied, connected, and/or allowed to interact with IT resources without appropriate departmental approval.
2. No hardware, software, or network infrastructure of any kind shall be deactivated, deleted, removed, or disabled from IT resources without appropriate departmental approval.
3. Staff shall use software obtained from sources outside the Department in compliance with licensing agreements.
4. Staff shall not distribute or disclose any software and related documentation developed by the Department without prior authorization.

C. Electronic Data

1. General Usage: Staff shall not download/upload non-work related electronic data files to IT resources or download/upload work related data files to personally-owned IT resources without prior review and approval of Technical Services and/or Security.
2. Copyrighted Materials: Staff shall not import, copy, store, or transmit copyrighted materials, without permission from the copyright owner. Even if materials are not marked with the copyright symbol, ©, staff should assume that materials are protected under copyright laws unless they explicitly state permission for their use.
3. Proprietary and Confidential Electronic Data
  - a) Proprietary and confidential electronic data includes (1) electronically stored juvenile information, including information stored in the North Carolina Juvenile Online Information Network (NC-JOIN), and (2) electronically stored personnel information, subject to specific statutory exceptions. Confidential information shall be accessed and disclosed with specific authorization and in adherence to the Department's "Confidentiality Agreement" (*Form DJJDP 19 001*) and State and federal law.
  - b) Staff shall safeguard Department-owned proprietary and confidential data as follows:
    - (1) Staff shall use only secure means to transmit proprietary or confidential data within the Department.

(a) A secure means of transmitting/receiving data automatically exists when an employee is routinely transmitting and receiving from one (1) state facility to another over the state network. However, when traveling and dialing in (connecting) to the state network from a non-Department facility like a motel, residence, etc., the Virtual Private Network (VPN) mode of operation on the laptop must be used to automatically encrypt data being sent or received.

(b) **E-mail transmission is not a secure means of transmitting data.**

(2) Staff shall allow only authorized persons access to Department-owned proprietary and confidential data.

(3) Staff shall distribute Department-owned proprietary or confidential data outside of the Department only as follows:

(a) According to established Department policies, guidelines, and procedures, or

(b) With authorization from the Department Data/Research Management, Communications Office, or Executive Management.

4. North Carolina State Network/Internet: Staff shall use the North Carolina State network and the Internet in compliance with Section II., A., and “General Use” of this policy.

#### D. Computer Accounts

1. Staff shall login to computers through the login screen using their assigned computer account information each time the computer is started.

2. Staff shall not share their assigned account information or personal passwords with other persons.

3. Staff shall not allow other persons to use their computer account to access IT resources.

4. Staff shall not leave written computer account information or personal passwords in a visible or easily accessible location.

*EXAMPLES: Leaving account information in a visible location would be a post-it note stuck to a computer monitor. Leaving account information in an easily accessible location would be written on a piece of paper placed under the keyboard.*

#### E. E-Mail

1. General Usage: Staff are prohibited from transmitting e-mails for the following purposes:

- a) To contact persons in the custody of a state, county, or federal correction system under any circumstance;
  - b) To communicate unauthorized and/or non-work related information to juveniles in the custody of the Department; or
  - c) To circulate unauthorized materials as identified in this policy.
- NOTE: Reference Section II., A., "General Use," (6) of this policy for a description of unauthorized materials.*

2. Department-wide E-mail Distribution List: The Department-wide e-mail distribution list may be used for Department business, and safety and security communications that apply to all staff. Requests for exceptions may be submitted to the Secretary, or his designee, for approval prior to distributing the communication.

3. Other E-mail Distribution Lists: Other e-mail distribution lists may be used as specified by the appropriate manager/supervisor.

4. All outgoing e-mail must contain the following disclaimer statement: *"Email correspondence to and from this address is subject to the North Carolina Public Records Law and may be disclosed to third parties by an authorized state official. Unauthorized disclosure of juvenile, health, legally privileged, or otherwise confidential information is prohibited by state and federal law. If you have received this e-mail in error, please notify the sender immediately and delete all records of this e-mail."*

### III. IT RESOURCE USAGE MONITORING AND ENFORCEMENT

A. The Department reserves the right to monitor, log, and report, with or without notice, all IT resource activity. This right includes monitoring the web pages that a staff member visits, and reading an e-mail sent by a staff member to ensure compliance with Department policy.

B. The Department reserves the right to identify and block access to an Internet site. Staff may submit requests for exceptions to the IT Help Desk for appropriate review and approval.

### IV. DOCUMENTATION

A. All Department supervisors shall ensure that each staff member under their supervision has signed the "Statement of Understanding Use of Information Technology Resources" (*Form DJJDP5 001*) and the "Confidentiality Agreement" (*Form DJJDP 19 001*) and shall place copies in the staff member's file, located at the staff member or supervisor's facility/office. The original shall be sent to the Policy Office in accordance with signature tracking procedures.

V. REPORTING SUSPECTED/OBSERVED COMPUTER VIRUSES, SPAM E-MAIL  
Staff shall immediately report any suspected or observed computer virus to the IT Help Desk via telephone. Staff shall not forward the suspected virus to the Help Desk.

- VI. REPORTING IT RESOURCE UNAUTHORIZED USE/MISUSE: Staff shall immediately report any suspected or observed unauthorized use and/or misuse of an IT resource to their departmental supervisor in accordance with *DJJD 8, Misuse and/or Theft of State Property*.
- VII. ATTACHMENTS
  - A. Statement of Understanding Use of Information Technology Resources (*Form DJJD5 001*)
  - B. Confidentiality Agreement (*Form DJJD 19 001*)