

**OKLAHOMA COUNTY JUVENILE BUREAU  
POLICY AND PROCEDURE MANUAL**

**CHAPTER THREE: PERSONNEL**

**POLICY 3.24 USE OF INTERNET/ EMAIL/ COUNTY COMPUTERS and  
CONFIDENTIALITY**

**PAGE 1 OF 6**

**I. Policy:**

The purpose of this procedure is to identify the circumstances under which Oklahoma County Juvenile Bureau (OCJB) employees may access the Internet through county computers, and define what OCJB considers acceptable use and conduct once an employee is connected to the network. This procedure communicates the OCJB's expectations with respect to what is, and is not, "acceptable use" and to minimize the risk of inappropriate behavior on the network. The OCJB protects the security and dissemination of information, as well as the access to and verification of data as it pertains to the privacy of juveniles. **(2-7078); (3-JDF-1E-08)**

**II. Procedures:**

OCJB has adopted and follows 2.20, "Computer Security", effective 09/01/13, as outlined in the Oklahoma County Employee Handbook.

A. Overview of the Internet

Although the Internet represents a potentially valuable resource, it also exposes the OCJB and its employees in an unprecedented and highly visible fashion. The Internet is a public forum, as opposed to a private or secure network. The County of Oklahoma may be held accountable for abusive, inappropriate, or unethical behavior of employees accessing the network. The protection of proprietary information, the isolation and security of internal systems and the productivity of the work force are of the utmost importance. All aspects of OCJB's Internet presence must be carefully managed to ensure that the OCJB and The County of Oklahoma's image is properly protected, its liability is limited and that access and use of the Internet by OCJB employees is suitable for business purposes and accomplished in a cost-effective manner.

B. Internet Privilege

Internet services are provided by the County of Oklahoma to support open communications, the exchange of information and the opportunity for collaborative, government-related work. OCJB encourages the use of electronic communications by its employees. Although access to information and information technology is

essential to the mission of the OCJB, use of Internet services is a revocable privilege.

- C. Employee Compliance; and Employee Acknowledgement of Receipt  
Employees will make a reasonable effort to inform themselves of this procedure and acceptable and unacceptable uses of the Internet in general. The burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to use. All new employees receive an overview of and copy of this policy. Employees will sign the "Acknowledgement of Receipt", Attachment A (3.24—A). All employees receive a copy of this policy anytime revisions are made, and will sign the "Acknowledgement of Receipt", Attachment A. (3.24—A)

- D. Employee Use  
Misuse or abuse of OCJB computer systems for tasks of a personal nature is prohibited.

1. Employee Etiquette  
Employees should know and follow the generally accepted etiquette of the Internet. For example:

- a). Use civil forms of communication;
- b). Respect the privacy of others;
- c). Respect the legal protection provided by copyright and license to programs and data;
- d). Respect the privileges of other users; and
- e). Respect the integrity of computer systems connected to the Internet.

2. Employee Agency Consideration  
Employees will avoid uses of the network that reflect poorly on the County of Oklahoma and on the OCJB.

3. Employee Ethical Behavior  
Existing rules, regulations and guidelines on the ethical behavior of OCJB employees and the appropriate use of County of Oklahoma resources also apply to the use of electronic communications systems such as the telephone, internet and e-mail access as provided by the County of Oklahoma.

- E. Information Exchange

1. Acceptable Uses  
Acceptable uses include but are not limited to:

- a). Communication and information exchange directly related to the mission, and work tasks of the OCJB;
- b). Communication and exchange for professional development, to update training or education, or to discuss issues related to the user's OCJB activities;
- c). Use in applying for or administering grants or contracts for OCJB research or programs;
- d). Use for advisory, standards, research, analysis, and professional activities related to the user's work tasks and duties;
- e). Announcement of new laws, procedures, policies, rules, services, programs, information or activities; or
- f). Any other governmental administrative communications not requiring a high level of security.

2. Unacceptable Uses

Unacceptable uses include, but are not limited to:

- a). Use of the Internet for any purpose which violates a federal or state law;
- b). Use for any for-profit activities unless specific to the mission, or duties of OCJB;
- c). Use for private business, including commercial advertising;
- d). Use for access and/or distribution of indecent or obscene material;
- e). Use of the Internet to access websites containing visual representations that contain actual or simulated sexual activity to include intercourse, sodomy (oral or anal), bestiality, sadomasochism, and child pornography is strictly prohibited and will result in immediate discharge from employment;
- f). Use for access to and/or distribution of computer games that have no bearing on the OCJB's mission. Games that help teach, illustrate, train, or simulate business-related issues may be acceptable;
- g). Use of Internet services to interfere with or disrupt network users, services, or equipment;
- h). Use to seek out information, distribute information, obtain copies of, or modify files and other data, which are private, confidential, or not open to public inspection or release;

- i). Use to copy software, electronic files, programs or data without a prior, good faith determination that such copying is permissible. Any efforts to obtain permission should be adequately documented;
- j). Employees misrepresenting themselves as other persons either on the Internet without the express consent of those other persons;
- k). Intentionally developing programs designed to harass other users, or infiltrate a computer or computing system, and/or damage or alter the software components;
- l). Use for fund raising or public relations activities not specifically related to OCJB activities; or
- m). Use to distribute personal opinion emails to groups of employees that is not directly related to accomplishing the mission and/or work tasks of the OCJB, such as political and/or religious messages. Engaging in discussions where disclaimers such as "this represents my personal opinion and not that of the OCJB and/or the County of Oklahoma" are prohibited.
- n). Allowing Residents/ Clients access to the Internet, except for educational or vocational testing under the management and control of an authorized instructor. Testing access will be site specific, under the direct supervision of an authorized instructor, with no access to the Internet beyond the test site. Physical and logical security will be imposed to restrict any unsupervised Resident/ Client access to any computer connected to the Internet.

3. Additional Guidelines

- a). Any software/files downloaded shall be virus checked prior to use. Please check with the County of Oklahoma Information Technology Division.
- b). Passwords associated with OCJB information systems will only be used on the authorized County of Oklahoma computer system. When setting up an account on a non-OCJB information system, passwords should be chosen that are different from ones used on the OCJB systems.
  - i). Use of the same password for both local and remote Internet-accessed systems is prohibited. If the password used at the Internet-accessed remote site were to be compromised, the different password used locally would still be secure.

- ii). Passwords should not be so obvious that others could easily identify them. Passwords should be changed at least every 90 days.
- c). A reasonable attempt will be made to complete the logoff or other termination procedure when finished using a remote, Internet-accessed system or resource. This will help prevent potential breaches of security.
- d). Electronic mail sent or received on the Internet cannot be expected to be secure.
- e). Employees utilizing electronic mail will ensure the electronic mail signature block does not include graphics, logos, clip art, quotes or any additional sayings. Messages containing confidential Resident/ Client or employee information shall include a confidentiality statement. The signature block will include the employee's name, title, work unit, work address, office phone and fax number. Default Microsoft Outlook settings for font, styles, colors and backgrounds will be used in both the body of the email and the signature blocks.
- f). The Internet connection is a shared resource. While routine electronic mail and file transfer activities will not normally impact others, large file transfers and intensive multimedia activities may impact the service levels of other users. Employees contemplating file transfers over 10 megabytes per transfer or interactive video activities should be considerate of other employees, and schedule these activities early or late in the day or after business hours. Such file transfers shall only be for OCJB business only and not for personal use.

### **III. Confidentiality**

- A. POLICY: It shall be the policy of the Bureau/Detention that all employees, volunteers, practicum students/interns, consultants and contract personnel shall adhere to Title 10 7305.1.3 C, concerning confidentiality of all information obtained as a result of employment or association with the Juvenile Bureau: (3-JDF-1C-22) (2-7044)

"All information obtained in discharge of official duty by an officer or other employee of the court shall be privileged and shall not be disclosed to anyone other than the judge and others entitled under this act to receive such information, unless and until otherwise ordered by the judge."

- B. POLICY: An employee may not disclose any information so defined by the Open Records Act, 51 O.S. 1985, Sec. 241.1 et. seq., to any unauthorized person without permission of the Department Director or County Officer. Requests for such information will be referred to the Director. An employee may not take any printouts, magnetic tapes, disks, cards, etc., which contain public or private information from any office, without prior permission from the Director. Any breach of confidentiality will be grounds for immediate termination.

Approved: \_\_\_\_\_

James L. Saffle, Director

Date

Attachment A (3.24 A): "Acknowledgement of Receipt", created 09/14

Honorable Lisa Tipping Davis  
District Judge  
Juvenile Division



James L. Saffle  
Director

**OKLAHOMA COUNTY JUVENILE BUREAU**  
*"Providing Opportunities for Success"*

**TELEPHONE, E-MAIL, INTERNET, AND VOICEMAIL EMPLOYEE**  
**ACKNOWLEDGEMENT FORM**

I have read and understand the Oklahoma County's Electronic Communication Policy included in the Oklahoma County Elected Official's Employee Personnel Policy Handbook. I understand that all electronic communication systems and all information transmitted by, received from, or stored in these systems are the property of Oklahoma County. I also understand that these systems, including facsimile, tele copier, telephone, voice-mail, copy machine, computer, Internet, E-mail, and telephone systems, are to be used primarily for job-related purposes and not form personal purposes, and that I have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt, or storage of information in this equipment.

I agree not to use a code, access a file, or retrieve any stored communication unless authorized. I acknowledge and consent to Oklahoma County monitoring my use of this equipment at any time, at its discretion. Such monitoring may include monitoring telephone communication, printing up and reading all E-mail entering, leaving, or stored in these systems as well as listening to my voice-mail messages. Each Oklahoma County Elected Official reserves and may exercise the right to review, audit, intercept, access, disclose, delete, and purge all messages or content created, received or sent over the Internet or E-mail access systems for any purpose. An employee's use of the Internet and E-mail systems grants management permission to review any and all transactions or sites.

I understand that unauthorized, excessive, or inappropriate use of any of the electronic communication systems may be grounds for discipline, up to and including discharge. I understand that this Acknowledgement Form will be placed in my personnel file.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Witness

\_\_\_\_\_  
Date

Distribution: Personnel File (Original)