



Employee and Non-Employee Acknowledgment of Confidentiality

Confidential case records.

OKDHS case records are confidential. Employees and non-employees are prohibited from accessing or viewing these records for any reason other than performance of assigned duties. Employees are prohibited from removing case files from any office outside of routine, official business processes without expressed consent from a supervisor.

Unauthorized disclosure of case records is prohibited by State and Federal law. Disclosure of certain records, such as records relating to child abuse and neglect, is also punishable as a crime under Oklahoma law. [10 O.S. §7107 and 56 O.S. §240.22C] Access to confidential databases, such as tax and earnings history, may not be used for any purpose other than performance of assigned duties. Unauthorized access or improper disclosure of case records or database information may result in disciplinary action, up to and including discharge from employment.

Computer and Internet usage.

OKDHS provides personal computers for staff use in the performance of their assigned job duties. In this regard, every employee must be aware of, and adhere to, the following restrictions and guidelines.

1. There is no expectation of privacy for use of an OKDHS computer for any purpose, whether business or personal. This may include, but is not limited to, the use of OKDHS network services local area network (LAN), Internet, including e-mail, and Web site browsing.
2. OKDHS may audit the use of any computer provided to any of its agents and employees to identify unauthorized activity. Audits review stored data, read and monitor electronic mail, record Web sites visited, and delete unauthorized files.
3. Uses of OKDHS computers for non-job-related activities must be minimal and must not diminish the number of actual hours worked or impede the employee's ability to complete tasks for which the employee is responsible.
4. Any action that threatens security or integrity of programs or data on any OKDHS computer must be avoided. Any action that might be in violation of any software license must be avoided.
5. Unacceptable use of OKDHS computers includes, but is not limited to:
 - displaying, viewing, storing, printing, or sending vulgar, offensive, or harassing material to anyone;
 - accessing sexually oriented Web sites, or storing, or viewing sexually oriented graphic images;
 - accessing sites for gambling, such as on-line casinos;
 - accessing sites to sell personal property, such as on-line auction services;
 - using OKDHS computers or equipment for outside business interests;
 - initiating or forwarding chain letters, or any non-job-related messages urging recipients to forward them to others;

- intentionally or recklessly introducing a virus or virus-like program onto an OKDHS computer;
- encrypting or password protecting data stored on OKDHS computers without prior written approval of the Data Services Division (DSD) and adherence to any conditions imposed upon such approval. Use of password protected data available in a read only status is permissible. See <http://infonet/office/dsd/ets/sec/docs/internetusagepolicy.htm> for a list of other approved uses of encryption and password protection;
- accessing confidential client records for purposes unrelated to performance of job duties;
- transferring confidential client records to persons unauthorized by law to receive such information;
- using software in such a manner as to violate copyright laws;
- loading personal copies of software not licensed to OKDHS or approved for use in OKDHS computers. A list of approved software is located at <http://infonet/office/dsd/ets/sec/docs/internetusagepolicy.htm>.
- loading, downloading, or using any software harmful to the operation of OKDHS computers; or
- using any screen saver not supplied with an OKDHS workstation.

Failure to abide by these restrictions and guidelines may result in disciplinary action, up to and including, termination from employment, based on the severity of the violation. Access to computers or certain computer functions, such as e-mail, LAN, or the Internet, may be suspended or denied at the sole discretion of OKDHS. **OKDHS reports any facts reasonably believed to be a violation of State or Federal criminal law to appropriate law enforcement authorities for prosecution.**

6. Access to the Internet from the OKDHS network is through a single access point.
7. An approved level of encryption must be used when transmitting confidential OKDHS data over the Internet, by use of Internet e-mail or file transfer, using DSD procedures. Transmission of confidential data over the Internet requires prior approval by the DSD Data Security Unit.

I acknowledge that I will comply with the restrictions and guidelines set forth above. I further acknowledge that I will abide by State and Federal laws regarding confidentiality of client records.

I understand that failure to comply with and sign acknowledgment of these terms may result in disciplinary action, up to and including, termination from employment, and prosecution of criminal violations.

_____	_____	_____
Employee signature	Title	Job code
_____	_____	_____
Employee printed name	User ID number	Date
_____	_____	_____
Non-employee signature	Title	Job code
_____	_____	_____
Non-employee printed name	User ID number	Date