

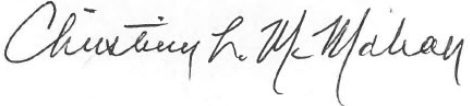



Oregon Juvenile Justice Information System Policy Statement

Subject: III — Governance and Administration

Section: A — Access and Security

Policy III-A-2 — JJIS User Security

 Christina McMahan, Co-chair JJIS Steering Committee	Effective Date:	6/1/2018
	Supersedes:	4/18/2012
	Date of Last Review/Revision:	5/25/2018
 Peter Sprengelmeyer, Co-chair JJIS Steering Committee	REFERENCE:	
	<ul style="list-style-type: none"> – OAR 416-180-0000: Administration of JJIS; Purpose – OAR 416-180-0050: Information Security – JJIS Policy: III-A-4: Privacy & Protection of Confidential Information in JJIS 	

PURPOSE:

To articulate security standards for access and use of the Oregon Juvenile Justice Information System (JJIS), to include clarification of standards for authorization and revocation of access; and consequences for violations of security.

DEFINITIONS:

JJIS User: an individual who is authorized to view or enter information in JJIS, JJPS, or JPAS

- **JJPS User:** a public safety agency employee who is authorized to access the Juvenile Justice Partner System (JJPS) to only view the status of youth cases and releasable, non-confidential information
- **JPAS User:** an OYA contracted service provider employee who is authorized to access the Juvenile Provider Access System (JPAS) to facilitate the referral, screening, and placement process

JJIS Youth Worker: a JJIS user who has an assigned youth caseload

JJIS Data Steward: OYA’s Information Systems Chief Information Officer, responsible for the high-level administration and security of JJIS

JJIS Security Officer: OYA staff member responsible for overseeing JJIS security protocols, consistent with JJIS policies and the direction of the JJIS Data Steward

Local JJIS Security Coordinator: an OYA or county primary or back-up contact for administering and supporting JJIS security guidelines

JJIS Internal Partners: Oregon Youth Authority and county juvenile departments whose employees directly record data, report information, or manage youth caseloads using JJIS

JJIS External Partners: other public and private agencies that work with youth served by the county juvenile departments and the Oregon Youth Authority and have been authorized to have access to JJIS

POLICY:

General Policy

Information in JJIS is confidential unless considered public information pursuant to Oregon Revised Statute (ORS) 192.410 to 192.505; 419B.035; 419A.255.

JJIS users will comply with all federal, state, and local laws regarding public information and confidentiality, as well as information technology standards set forth by the Oregon Legislature, the Department of Administrative Services, and the Oregon State Police Criminal Justice Information Services Division

JJIS data is under the jurisdiction of all county juvenile departments and the Oregon Youth Authority. JJIS users have an ethical responsibility to the multiple jurisdictions whose data are contained in JJIS.

To protect the integrity of the system, JJIS users will conform to system security measures, as defined by JJIS policies and procedures and implemented at the local level through related procedures.

JJIS users are responsible for all transactions entered under their JJIS log-on and will not share their user name or password with anyone.

To preserve the anonymity and confidentiality of youth information, users will not leave their computer or electronic device screen unattended or accessible for unauthorized use or viewing by the public or any other unauthorized persons.

JJIS users are required to agree to security declarations included in a JJIS user security agreement prior to receiving access to JJIS and on an annual basis. Access to JJIS may be revoked if a user does not adhere to the standards in this policy or the user agreement.

Access to Youth Records

Workers who are assigned to work with a youth have access to the youth record consistent with the worker's security roles. Workers are considered assigned to a youth when they:

- are recorded as an active worker on the youth record;
- work in the same office as the assigned worker; or
- work in a facility in which the youth is currently admitted and they have a specific direct working relationship with that youth.

A worker may also have an otherwise authorized work-related reason to access a specific youth record or specific information on a youth's record. However, authorized work-related reasons do not extend to all

youth in the office or facility where a worker works. Accessing a case where the worker does not have a direct relationship to work with that specific youth is not considered an authorized job task, and may be subject to a JJIS security violation review.

Temporary Assignment to Youth Records

Workers who are not assigned to work with a youth may have a legitimate need to view and update youth information consistent with their security roles (e.g., detention intake screening, close custody transport, business analysis, or user assistance). Workers who need access to the record of a youth to whom they are not assigned may grant themselves temporary assignment for 24 hours. JJIS tracks temporary assignments.

Confidentiality and Appropriate Use

JJIS information will be used only for legitimate law enforcement and juvenile justice purposes, or as otherwise allowed by state and federal statute. JJIS information should be conveyed only in a secure and appropriate manner.

No individual can seek, obtain, use, or release information from JJIS for private or personal reasons.

Viewing information in JJIS is the equivalent of viewing information in a hard copy file. JJIS users will seek, obtain, and use only the minimum amount of information needed to accomplish an authorized job task.

Some information in JJIS can be marked as protected information. Use of the protection indicator does not restrict access to cases, but it does initiate an automatic entry on log that tracks access to protected information. (See JJIS policy on “Privacy and Protection of Confidential Information”.)

Users seeking public information for uses other than an authorized job task should request and obtain the information from their local JJIS Security Coordinator. The Security Coordinator will review the request and respond consistent with local and JJIS policies on public information.

JJIS information can only be viewed and released subject to agency and JJIS policy. Unless otherwise provided by JJIS policy, information on youth with active cases should be released only by the agency with jurisdiction or physical custody, and in accordance with prevailing state and federal statutes. Disclosure of information on youth with a closed case is also subject to agency policy and must be in accordance with prevailing state and federal statutes. Unless otherwise provided by JJIS policy, confidential information should be released only by the agency that entered the information into JJIS.

Any information in JJIS that relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual (known as “health information”) is considered confidential under the federal Health Insurance Portability and Accountability Act (45 CFR Parts 160 and

164) (HIPAA). Disclosure of health information which is not otherwise allowed or required by state or federal law may be a serious violation and subject to criminal investigation and prosecution by the State of Oregon and by the federal government.

Electronic Disclosure of JJIS Information

Some JJIS features create automatic email notifications to designated users, (for example, Youth Incident Report notifications). JJIS users will adhere to JJIS and local agency policies regarding access, disclosure, confidentiality, and security when retrieving and disclosing any juvenile records contained in JJIS into a report, document, screen print, email, or other electronic format.

JJIS security protections that safeguard confidential juvenile records do not exist in various email and external electronic systems such as smartphones and tablets. Dissemination of these records by other electronic format increases a risk of inappropriate disclosure. To limit this risk, juvenile records referenced in an email or other electronic format will adhere to the following guidelines:

- Identity of the Recipients

When an email contains youth information obtained from JJIS, whether or not it contains personally identifiable information about a youth, the names of the sender and all recipients of the email must be clearly visible on the email. Any group distribution must clearly identify the members of the distribution group. The use of blind copy, generic group distribution, or any other means that masks the identity of a recipient is prohibited.

- Content Guidelines

Confidential youth information will not be disclosed via text messaging.

Medical information will not be sent by email, text messaging, or any other electronic format unless that format adheres to federal and state requirements and includes adequate transmittal protections, such as encryption.

Local agency policy may have additional guidelines and may be more restrictive.

Conflict of Interest and Notification of Supervisor

Employees are prohibited from using the JJIS system or data for their own interest, advantage, personal gain, or for any private purpose.

To support appropriate use and avoid potential conflicts of interest, employees with access to JJIS will notify their immediate supervisor if expected to work on a case where the employee has a close personal relationship with a youth or an associate of a youth in JJIS.