Interstate Commission for Juveniles

Privacy Policy

Juvenile Interstate Data System (JIDS)

Version 1.0

Approved:
February 23, 2012

1.0 Statement of Purpose

The goal of establishing and maintaining the JIDS is to further the following purposes of the Commission:

A. Increase public safety and improve national security;

B. Minimize the threat and risk of injury to specific individuals; including but not limited to: law enforcement and others responsible for public protection, safety, or health;

C. Minimize the threat and risk of damage to real or personal property;

D. Protect individual privacy, civil rights, civil liberties, and other protected interests;

E. Protect the integrity of the juvenile justice system processes and information;

F. Support the role of the juvenile justice system in society;

G. Promote information legitimacy and accountability;

H. Not unduly burden the ongoing business of the juvenile justice system;

I. Make the most effective use of public resources allocated to juvenile justice agencies; and

J. Maximize the efficient implementation and administration of the Interstate Compact for Juveniles and its authorized bylaws, rules and policies.

2.0 Accountability

A. The existence of JIDS will be made public and the system's policies on protection of privacy, civil rights, and civil liberties will be made available to the public upon request.

B. ICJ will adopt provisions to ensure accountability for compliance with all applicable laws and policies in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

3.0 Definitions

A. "ICJ" means the Interstate Commission for Juveniles.

B. "JIDS" means the Juvenile Interstate Data System.

C. "Information" means any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

D. "Law" means any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal agencies, officials and courts.

E. “Member Agency” means those states, as defined in the Interstate Compact for Juveniles (“Compact”), including their political subdivisions, to which states are members of the Interstate Commission for Juveniles and the primary users of the JIDS system.

F. “Participating Agency” means both member agencies and other justice system partners who share or use the JIDS system.

G. “Public” means:

1) Any person and any for-profit or nonprofit entity, organization, or association;
2) Any governmental entity for which there is no existing specific law authorizing access to the participating agency’s information;
3) Media organizations; and
4) Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the participating agency.

H. “Public” does not include:

1) Employees of the participating agency;
2) People or entities, private or governmental, who assist the agency in the operation of the justice information system; and
3) Public agencies whose authority to access information gathered and retained by the participating agency is specified in law.

The bulk release of information to either the public, private, or non-profit agencies is permitted only if they are authorized by law and approved in advance by the ICJ.

4.0 Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

A. ICJ and all participating agencies, employees, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

B. ICJ will adopt internal operating policies requiring compliance with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system.

C. ICJ will conduct periodic audits to measure compliance with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system.

D. The Health Insurance Portability and Accountability Act (“HIPAA”) exempts certain disclosures of health information for law enforcement purposes without an individual’s written authorization. The various conditions and requirements concerning these exempt disclosures are contained in the regulatory text of the HIPAA privacy rule and may be found at 45 C.F.R 164 et. seq. Under these provisions protected health information may be disclosed for law enforcement purposes when such disclosures are required by law. Thus, disclosure of protected health information required to be furnished by or received

from member agencies which administer the Compact acting pursuant to the provisions of the Compact and its authorized rules is permissible.

5.0 Expectations Regarding Information Gathered and Shared

A. Member agencies will adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to:

1) Seek or retain only information that is legally permissible for the participating agency to seek or retain under laws applicable to the participating agency;
2) Use only lawful means to seek information;
3) Seek and retain only information that is reliably accurate, current, and complete;
4) Take appropriate steps when merging information about a juvenile from two or more sources, to ensure that the information is about the same juvenile;
5) Investigate in a timely manner any alleged errors and correct information found to be erroneous;
6) Retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to the administration of the Compact;
7) Maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions;
8) Collect and analyze information in a manner that conforms to generally accepted practices;
9) Establish procedures that comply with the policies and procedures of the ICJ for accessing information through the participating agency;
10) Allow only authorized users to access the information in JIDS and only for purposes related to the performance of their official duties;
11) Share information with authorized users of other justice system partners based only on a “right-to-know” and a “need-to-know” basis; and
12) Establish and comply with information retention and destruction schedules.

6.0 Sharing Information with Other Justice System Partners

A. When there is a question or inquiry about shared data, a participating agency will make information available in response to a query either by:

1) Providing the requested information directly;
2) Responding with the contact information of a person in the responding agency whom the individual making the query can contact;
3) Having a person in the responding agency contact the individual making the query; or
4) Indicating that no information is available.

7.0 Disclosure of Information According to the Originating Agency’s Access Rules

A participating agency will not disclose information originating from another participating agency except as provided for in this agreement or in the operational policies of JIDS.

8.0 Reporting Possible Information Errors to the Originating Agency

When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated in writing to the JIDS Administrator at the ICJ's National Office, who will then work with the submitting agency to make the necessary correction.

9.0 Expectations Regarding Accountability and Enforcement

A. Participating agencies will adopt and comply with internal policies and procedures requiring the agency, its personnel, contractors, and users to:

1) Have and enforce policies for discovering and responding to violations of agency policies and this policy, including taking appropriate action when violations are found;
2) Provide training about the agency's requirements and policies regarding information collection, use, and disclosure to personnel authorized to use JIDS;
3) Make available to the public the agency's internal policies and procedures regarding privacy, civil rights, and civil liberties;
4) Cooperate with periodic, random audits by representatives of the ICJ; and
5) Designate an individual within the participating agency to receive reports of alleged errors in the information that originated from the participating agency.

10.0 Enforcement of Provisions of Information Sharing Agreement

A. If a participating agency fails to comply with the provisions of this agreement or fails to enforce provisions in its local policies and procedures regarding proper collection, use, retention, destruction, sharing, disclosure, or classification of information, the ICJ may:

1) Suspend or discontinue access to JIDS by a user in the offending agency who is not complying with the agreement or local policies and procedures;
2) Suspend or discontinue the offending agency's access to JIDS; or
3) Offer to provide an independent review, evaluation, or technical assistance to the participating agency to establish compliance.

11.0 Information Sought and Retained

A. Participating agencies will seek or retain only information that is:

1) Relevant to the juvenile compact process and the return of runaways, escapees, absconders and delinquent juveniles.

2) Relevant to the investigation and prosecution of suspected juvenile offenses; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of juvenile offenses or that is useful in analysis of juvenile offenses or in the administration of the juvenile justice system.

3) Collected by participating agencies on specific juveniles, consisting of official identifiable descriptions and notations of arrests, detentions, warrants, complaints, indictments, information, or other formal charges, and any disposition relating to

these charges, including acquittal, sentencing, pre- or post-conviction supervision, correctional supervision, and release.

4) Participating agencies will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any juvenile or the race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation of such juvenile unless such information is needed by the participating agency:

    i. To identify a juvenile;
    ii. In order for the agency to operate effectively; or
    iii. To provide services to the juvenile.

B. The participating agency shall keep a record of the source of all information retained by the participating agency.

12.0 Classification of Information Regarding Limitations on Access and Disclosure

A. At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

1) Protect confidential sources and police undercover techniques and methods;
2) Not interfere with or compromise pending investigations;
3) Protect a juvenile's right of privacy and civil rights; and
4) Provide legally required protection based on the status of an individual as victim.

B. The classification of existing information will be reevaluated whenever:

1) New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
2) There is a change in the use of the information affecting access or disclosure limitations.

C. The access classifications will be used to control:

1) What information a class of users may access;
2) What information a class of users can add, change, delete, or print; and
3) To whom the information can be disclosed and under what circumstances.

13.0 Information Quality

A. Participating agencies will make every reasonable effort to ensure that information sought or retained is:

1) Derived from dependable and trustworthy sources of information;
2) Accurate;
3) Current;
4) Complete, including the relevant context in which it was sought or received and other related information; and
5) Merged with other information about the same juvenile only when the applicable standard has been met.

B. Participating agencies will make every reasonable effort to ensure that only authorized users are allowed to add or change information in the system.

C. Participating agencies will make every reasonable effort to ensure that information will be deleted from the system when the agency learns that the:

1) Information is erroneous, misleading, obsolete, or otherwise unreliable;
2) Source of the information did not have authority to gather the information or to provide the information to the participating agency; or
3) Source of the information used prohibited means to gather the information.

14.0 Collation and Analysis of Information

A. Information sought or received by participating agencies or from other sources will be analyzed by qualified individuals to further prevention of juvenile offenses, enforcement, or prosecution objectives and priorities established by participating agencies.

B. Information sought or received by participating agencies or from other sources will not be analyzed or combined in a manner or for a purpose that violates Section *15.0 Merging of Information from Different Sources.*

15.0 Merging of Information from Different Sources

A. Information about a juvenile from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same juvenile.

B. The set of identifying information sufficient to allow merging will consist of at least four of the fields, including: first name, last name, date of birth, JIDS identifier and/or sending state identifier.

16.0 Sharing Information within the Agency and With Other Justice System Partners

A. Access to information retained by JIDS will be provided only to member agencies or other governmental agencies that are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with the law and procedures applicable to participating agencies for whom the person is working. The person who received, reviewed, or added information to the system may be authorized to view the information he or she provided regardless of the type of access associated with the information or the contributor's access authority.

B. When there is a question or inquiry about shared data, a participating agency will make information available in response to a query either by providing the requested information directly or by having a person in the responding agency contact the individual making the query.

C. An audit trail will be kept of access by or dissemination of information to such persons.

17.0 Sharing Information with Public Protection, Safety, or Public Health Agencies

A. Information retained by JIDS may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws regulations and procedures. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of juvenile offense intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

B. The ICJ shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

C An audit trail will be kept of the access by or dissemination of information to such persons.

18.0 Sharing Information for Specific Purposes

A. Information gathered and retained by JIDS may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

B. The ICJ shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

C. An audit trail will be kept of the requests for access and of what information is disseminated to such persons.

19.0 Disclosing Information to the Public

A. Information gathered and retained by JIDS may be disclosed to a member of the public only if the information is defined by law to be a public record and is not exempt from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to participating agencies for this type of information.

B. The ICJ shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

C. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

20.0 Disclosing Information to the Juvenile about Whom Information Has Been Gathered

A. Upon satisfactory verification of his or her identity and subject to the conditions specified in (B), a juvenile is entitled to know the existence of and to review the information about him or herself that has been gathered and retained by JIDS. The juvenile may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. A participating agency's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the juvenile.

B. The existence, content, and source of the information will not be made available to a juvenile when:

1) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
2) Disclosure would endanger the health or safety of an individual, organization, or community;
3) The information is considered criminal intelligence; or
4) The information is considered to be victim sensitive.

C. If a juvenile has objections to the accuracy or completeness of the information retained about such person, the ICJ will inform the juvenile of the procedure for requesting review of any objections. The juvenile will be given reasons if a request for correction is denied.

D. The ICJ will charge a $25.00 fee to those requesting information.

E. A record will be kept of all requests and of the information that is disclosed to a juvenile.

21.0 Review of Information Regarding Retention

A. Information will be reviewed periodically for purging.

B. When information has no further value or meets the criteria for removal under applicable law or ICJ Rules, it will be purged, destroyed, deleted, or returned to the submitting source.

22.0 Destruction of Information

A. Information in JIDS will not be purged, destroyed, deleted or returned without the written permission of the agency that submitted the information and in accordance with ICJ Rules.

B. Notification of proposed destruction or return of records will be provided to the agency submitting the information.

C. A record that information has been purged or returned shall be maintained by the ICJ.

23.0 Information System Transparency

A. The JIDS Privacy Policy is available to the public on request and on the ICJ website.

B. The Compact Commissioner in each state is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in JIDS and will provide to the public the contact information.

24.0 Accountability for Activities

A. The primary responsibility for the operation of JIDS, including operations; coordination of personnel; receiving, seeking, retaining and evaluating information quality; the analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy are assigned to the Commission's Executive Director.

B. The ICJ will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with industry standards.

C. JIDS will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

D. The ICJ will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy, industry standards and applicable law.

E. The ICJ will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy.

F. The ICJ will periodically conduct audits and inspections of the information contained in JIDS. The audits will be conducted randomly by a designated representative of the participating agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

G. The ICJ will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

H. The ICJ will notify a juvenile about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and to reasonably restore the integrity of JIDS.

25.0 Enforcement

A. If a user is suspected of or found to be in non-compliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the participating agency or the ICJ will:

1) Suspend or discontinue access to information by the user;
2) Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;
3) Apply other sanctions or administrative actions as provided in the participating agency's personnel policies;
4) Request the participating agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or
5) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

26.0 Training

A. Member agencies will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

1) Its personnel;
2) Personnel providing information technology services to the agency;
3) Staff in other public agencies or private contractors providing services to the agency; and
4) Users who are not employed by the agency.

B. The training program will cover:

1) Purposes of the privacy, civil rights, and civil liberties protection policy;

2) Substance and intent of the provisions of the policy relating to collecting, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;
3) The impact of improper activities associated with information accessible within or through the agency; and
4) The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

Juvenile Interstate Data System
Interstate Commission for Juveniles

END USER AGREEMENT

This JIDS End User Agreement ("Agreement") governs access privileges and the use of the Juvenile Interstate Data System. By way of this agreement the Interstate Commission for Juveniles ("ICJ") grants you, and you alone, electronic access to JIDS. Access is granted solely for use in accordance with the conditions and limitations outlined in this Agreement and the JIDS Privacy Policy ("Privacy Policy"). By signing this Agreement, you acknowledge that you have received, read and understand both the Agreement and the Privacy Policy and agree to comply with the specified conditions and limitations and any other included directive on the use and operation of JIDS.

If you cannot agree with the conditions specified in either this Agreement or the Privacy Policy, you will not be granted access to JIDS. Your failure to adhere to the conditions outlined may result in the suspension or termination of privileges without notice.

C O N D I T I O N S

By signing this Agreement you agree to the following conditions:

1. You have read and understand both this Agreement and the Privacy Policy.
2. The information provided in your application is true and accurate.
3. Access to JIDS is necessary to the performance of your duties.
4. Your right to use JIDS is exclusive to you. You may not authorize others to use your access.
5. You shall not use or divulge JIDS data for your personal interest, gain or exploitation or for the personal interest, gain or exploitation of any other individual, and shall not be assigned or otherwise transferred to any other person.
6. When using JIDS you shall not leave it unattended in areas where it might be accessed by unauthorized individuals.
7. You shall not access JIDS on public computers.
8. You shall not use JIDS on unsecured wired or wireless access points or connections.
9. You shall not divulge JIDS data to any person not authorized to receive it.
10. You shall not copy, reproduce, duplicate, modify, adopt or lend, sell or otherwise transfer, in whole or part, any information contained in JIDS, except for the specific business use authorized by ICJ.
11. All information you enter or attach is true, accurate, verified, current and complete to the best of your knowledge.
12. You agree not to disrupt, interfere, alter or tamper with any information or materials associated with JIDS use.
13. You agree to report any suspicious activity or known security or user violations to the National Office for the Interstate Commission for Juveniles. You agree to in no way change JIDS software, or to in any way decompile, disassemble or imitate any part of JIDS software.

INTERSTATE COMPACT FOR JUVENILES

JIDS USER ACCEPTANCE AGREEMENT

FIRST NAME: _____ LAST NAME: _____

USER NAME (EMAIL ADDRESS): _____

ROLE: _____ STATE: _____ STATUS: _____

By selecting the "I Accept" box, you acknowledge that you have read the Juvenile Interstate Data System (JIDS) Privacy Policy and User Acceptance Agreement and agree to be bound by the terms and conditions set forth. You agree to use JIDS for lawful purposes only and you acknowledge that your failure to do so may subject you to civil and criminal liability. If you do not agree to the terms and conditions of this agreement, you may not access, view, obtain services from, or otherwise use JIDS.

I ACCEPT ☐ DATE ACCEPTED: _____

By selecting the "I Accept" box below, you acknowledge that you have also received the permission of your state's compact administrator or designee to access JIDS.

I ACCEPT ☐ DATE ACCEPTED: _____