SECTION: 200.750
SUBJECT: Privacy Policy and Use of Personally Identifiable Information

POLICY

This policy establishes minimum requirements for the collection, access, use, transmission, storage, retention, disclosure, and destruction of personally identifiable information (PII) handled by the Dane County Sheriff's Office.

This policy is intended to:

- protect the privacy and security of PII;
- support compliance with grant requirements, county policy, and applicable law;
- reduce the risk of unauthorized access, use, or disclosure;
- establish staff responsibilities and rules of conduct; and
- promote consistent handling practices across Sheriff's Office divisions, units, programs, and operations.

This policy applies to:

- all Dane County Sheriff's Office employees;
- temporary employees, interns, volunteers, and trainees;
- contractors, consultants, vendors, and sub recipients with access to Sheriff's Office PII;
- sworn and civilian personnel;
- all formats of PII, including paper, verbal, electronic, photographic, scanned, audio, video, and data extracts; and
- all Sheriff's Office divisions, facilities, grant-funded programs, and systems in which PII is collected, maintained, used, or disclosed.

DEFINITIONS

Personally identifiable information (PII) means information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

PII includes, but is not limited to:

- full name;

- alias when linked to an identifiable individual;
- date of birth;
- home, mailing, or email address;
- telephone number;
- Social Security number;
- driver's license number or state identification number;
- passport number;
- financial account or payment card information;
- taxpayer identification number;
- biometric information;
- medical, treatment, or disability information when linked to an identifiable person;
- resident booking, resident incident(s), complaint(s), or case numbers when tied to a person;
- photographs, recordings, or documents identifying a person; and
- any combination of data elements that permits identification of a specific individual.

Sensitive PII includes PII that presents a heightened risk of harm if improperly accessed, used, or disclosed, including but not limited to Social Security numbers, driver's license numbers, financial account data, authentication credentials, medical information, victim information, juvenile information, and information protected by law, court order, or policy.

PROCEDURE

Personnel shall collect, access, use, maintain, share, and dispose of PII only to the extent necessary to carry out authorized official duties and only in accordance with law, this and other applicable policies,, grant requirements, and records retention obligations.

No workforce member may access, use, copy, discuss, transmit, alter, or disclose PII for personal reasons, curiosity, convenience, or any other unauthorized purpose.

Roles and Responsibilities

All Personnel with access to PII shall:

- protect PII from unauthorized access, use, disclosure, or loss;
- access only the minimum information necessary to perform assigned duties;
- comply with all applicable confidentiality, records, security, and technology policies;
- complete required privacy/security training;
- immediately report suspected or actual improper access, disclosure, or loss; and
- follow records retention and secure disposal requirements.

Supervisors

Supervisors shall:

- ensure personnel understand and comply with this policy;
- authorize access only where operationally necessary;
- monitor compliance within their units;
- ensure corrective action is taken when issues are identified; and
- notify appropriate command staff and support units of incidents or risks.

Records Custodian / Designee

The records custodian or designee shall:

- support lawful review and release of records;
- coordinate redaction and disclosure decisions as appropriate;
- assist in retention and records management compliance.

Information Technology

County IT personnel assigned to the Dane County Sheriff's Office shall:

- implement and maintain reasonable technical safeguards;
- support access controls, authentication, logging, and secure transmission methods;
- assist in incident investigation and containment; and
- coordinate technical remediation when needed.

Data Minimization and Collection

Personnel shall collect only the PII reasonably necessary for legitimate purposes.

PII shall not be collected "just in case" or for undefined future use.

Access Control

Access to PII shall be limited to personnel with a legitimate need to know based on assigned job duties.

Personnel shall not browse, search, or retrieve PII records out of curiosity or for non-business reasons.

Verbal Handling

Personnel shall take reasonable steps to prevent unauthorized verbal disclosure of PII.

Examples include:

- avoiding case discussions in public spaces, hallways, elevators, lobbies, or over open radio channels when unnecessary;
- verifying the identity and authority of callers before releasing information;
- lowering voices or moving to private areas when discussing sensitive matters; and
- limiting voicemail content containing sensitive PII.

ELECTRONIC TRANSMISSION

PII shall be transmitted electronically only when necessary for official business and by approved methods.

Email

- When sending PII by email, personnel shall:
- confirm recipient addresses before sending;

Text Messaging and Messaging Applications

- PII shall not be sent by text message or messaging application unless:
  - the platform is county-approved for that purpose;
  - the transmission is necessary for official operations; and
  - the method provides appropriate security and retention controls.

Fax

If faxing PII is necessary:

- confirm the destination number;
- use a cover sheet stating the material may be confidential;
- verify the intended recipient is available when appropriate; and
- promptly retrieve incoming faxed materials.

Portable Media

- PII shall not be stored on portable media or removable devices unless specifically authorized and protected using approved safeguards.

Artificial Intelligence (AI)

- Sheriff's Office staff shall use only County approved AI applications.
- PII shall not be used/uploaded into County approved AI applications.
- The use of other AI applications or websites, not approved by County IT is forbidden.

Remote Access and Mobile Work

Personnel accessing PII remotely or in the field shall:

- use approved devices, systems, and remote access methods;
- avoid viewing or discussing PII where unauthorized persons may observe or overhear;
- secure laptops, phones, tablets, and paper files in vehicles and field settings;
- log off or lock devices when unattended; and
- report lost or stolen devices or records immediately.

PII shall not be downloaded, printed, or locally stored on personal devices unless expressly authorized.

Paper Records

Paper records containing PII shall be:

- stored in secure offices, file rooms, cabinets, or controlled-access areas;
- transported only when necessary;
- kept under staff control when in use;
- shielded from view by unauthorized persons; and
- promptly returned to secure storage after use.

Stacks of records containing PII shall not be left on counters, printers, desks in public-facing areas, conference rooms, or vehicles without protection.

System Security and Technical Controls

Units and personnel shall comply with County and Sheriff's Office technical requirements for systems containing PII, including:

- password and authentication requirements;
- access logging where available;
- software update and patch requirements;
- malware protection;
- approved storage locations;
- approved file-sharing and collaboration tools; and
- restrictions on local or unapproved cloud storage.

Disclosure to Other Agencies or Third Parties

PII may be disclosed outside the Sheriff's Office only when:

- the disclosure is authorized by law;
- the disclosure is required for official operations.

Before disclosing PII externally, staff should evaluate:

- identity of the requester;
- legal basis for disclosure;
- minimum necessary scope of disclosure;
- whether redaction is required;
- whether the disclosure should be documented; and
- whether a data-sharing agreement, confidentiality provision, court order, or release applies.

Questions about external disclosure should be directed to a supervisor, records custodian, legal counsel, or other designated authority before release.

PUBLIC RECORDS REQUESTS

All requests for records shall be handled in accordance with Sheriff's Office records procedures and Wisconsin public records requirements.

Personnel shall not independently release records containing PII in response to a records request unless authorized to do so.

Contractors, Vendors, and Sub recipients

No contractor, vendor, consultant, evaluator, volunteer, intern, or sub recipient shall be granted access to PII unless:

- the access is necessary for authorized work;
- appropriate approvals have been obtained;
- confidentiality and data protection terms are in place where required; and
- the person or entity has been informed of applicable restrictions.

Contracts and agreements involving PII should address, as applicable:

- permitted use;
- access limitation;
- storage and security requirements;
- incident reporting;
- return or destruction of data;
- audit rights; and
- compliance with applicable law and policy.

RETENTION AND SECURE DESTRUCTION

Records containing PII shall be retained in accordance with applicable records schedules, litigation holds, operational requirements, evidentiary needs, and grant conditions.

Personnel shall not place records containing protected PII in ordinary trash or unsecured recycling.

INCIDENT REPORTING AND RESPONSE

Immediate Reporting

Personnel shall immediately report any known or suspected:

- unauthorized access to PII;
- unauthorized disclosure of PII;
- loss, theft, or misdirection of records or devices containing PII;
- phishing or compromise involving accounts that may expose PII;
- improper posting, attachment, or transmission of PII; or
- other event that may compromise confidentiality, integrity, or availability of PII.

Reporting Chain

Reports shall be made immediately to:

- the employee's supervisor;
- command staff, if appropriate;
- records, IT, security, grants, or privacy-designated personnel, as applicable; and
- any other reporting point required by county policy or incident response procedure.

Containment

Personnel shall take reasonable immediate steps to contain the incident, such as:

- recalling email where feasible;
- contacting unintended recipients and instructing them not to use or further disclose the information;
- securing exposed records;
- disconnecting compromised devices if directed; and
- preserving evidence for investigation.

Investigation and Follow-Up

The Sheriff's Office will investigate, document, and address incidents in coordination with appropriate county departments and legal or technical staff. Notification, mitigation, corrective action, and documentation shall occur as required by law and policy.

TRAINING

All personnel with access to PII shall complete required County and State provided/approved training regarding privacy, security, records, and acceptable-use training, such as annual NeoGov training, and biennial TIME system recertification :

- at onboarding or before access is granted;
- periodically thereafter as required; and
- when significant legal, policy, procedural, or system changes occur.

Supervisors may require supplemental unit-level training for high-risk functions.

AUDITING AND MONITORING

The Sheriff's Office may monitor access to systems and records containing PII and may audit compliance with this policy, technology policies, records procedures, grant conditions, and related requirements.

Personnel should have no expectation of privacy in the use of county systems for official business beyond protections provided by law and policy.



QUESTIONS AND ESCALATION

Personnel who are uncertain whether PII may be collected, used, shared, released, transmitted, or destroyed in a particular circumstance shall pause and seek guidance before proceeding.

Questions should be directed to:

- Immediate supervisor;
- Division Command;
- Records Custodian or designee;
- Grant/Program Administrator;
- Corporation Counsel;
- Information Technology/security staff; or
- other designated privacy or compliance contact.

RELATED DOCUMENTS

This policy should be read together with, as applicable:

- county records retention schedules and records procedures;
- county information technology and acceptable-use policies;
- public records procedures;
- grant conditions and grant agreements;
- applicable confidentiality laws and regulations; and
- division-specific procedures governing law enforcement, jail, medical, victim, juvenile, or treatment information.

REVIEW AND REVISION

This policy shall be reviewed periodically and revised as necessary to reflect changes in law, operations, grant requirements, county policy, security standards, or organizational structure.

RELATED DCSO POLICIES

Administrative Practice Manual: Proper Use of Computer Equipment, Software, and Connectivity

830.01 Computer Use Policy

830.03 TIME System

830.04 Mobile Data Computer

HISTORY

Date	By	Note
11.18.2026	Administration	New Policy