MIDDLETON POLICE DEPARTMENT	DATE **February 23, 2013**	POLICY **10.1.01**
SUBJECT: **Records**	REVIEWED May 18, 2017	

Refer to: 19.34(1), 19.35, 19.356, 19.36, 48.396, 165.55, 165.83(2)(a), 165.84(1), 938.02(1), 938.19, 938.02(10m), 938.396, 18 U.S.C.§ 2721, OP.55.66
History: 1995, 2/2013, 04/2015, 09/2015, 05/2016, 05/2017
WILEAG (5th Ed.) Standards: **10.1.1** (10.1.1.1; 10.1.1.2; 10.1.1.3); **10.1.7**; **10.1.9;** **10.1.10** (10.1.10.1; 10.1.10.2; 10.1.10.3; 10.1.10.4; 10.1.10.5), **10.2.2**

Contents

PURPOSE

The purpose of this policy is to provide guidelines on the proper procedures to collect, maintain, separate, secure, and avail reports and records of the Middleton Police Department.

POLICY

It is the policy of the Middleton Police Department that all records and reports are maintained in an orderly manner and that the department takes privacy and security precautions to ensure the protection of all records and confidentiality of citizens. It is the responsibility of the Records Bureau to process, store, and maintain reports in an accurate and timely manner. It is the responsibility of the Office Manager's office to process, store, and maintain departmental administrative records in an accurate and timely manner.

DEFINITIONS

Adult means a person who is 18 years of age or older, except that for purposes of investigating or prosecuting a person who is alleged to have violated any state or federal criminal law or any civil law or municipal ordinance, "adult" means a person who has attained 17 years of age [938.02(1)].

DPPA means the Driver's Privacy Protection Act which was enacted in 1994 and codified at 18 U.S.C.§ 2721, to protect people from the personal dangers resulting from the disclosure of sensitive personal information and highly restricted personal information by governmental entities to third parties.

Juvenile means a person who is less than 18 years of age, except that for purposes of investigating or prosecuting a person who is alleged to have violated a state or federal criminal law or any civil law or municipal ordinance, "juvenile" does not include a person who has attained 17 years of age [938.02(10m)].

Motor Vehicle Record in the context of the DPPA means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.

Offense means an act committed by a person who has attained the age of 10 that is a felony, misdemeanor, or ordinance violation.

Personal Information in the context of the DPPA means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

Record means any material on which written, drawn, printed, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics, which has been created or is being kept for official purpose or function of the department is a record. "Record" includes, but is not limited to, handwritten, typed or printed pages, maps, charts, photographs, films, recordings, tapes, (including computer tapes and disks and files), and computer printouts. "Record" does not include drafts, notes, preliminary computations and like materials prepared for the originator's personal use or prepared by the originator in the name of a person for whom the originator is working, materials which are purely the personal property of the custodian or employee and have no relation to his or her office or job; materials to which access is limited by copyright, patent, or bequest; and published materials in the possession of the department which are available for sale, or which are available for inspection at a public library.

RMS means records management system. RMS is an agency-wide computer system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to police operations. RMS records are to be maintained indefinitely. The department currently utilizes the Global Justice records management system.

PROCEDURE

Security

All paper police records are located within the physically secure restricted access area of the police department and are accessible only by police employees. Access to the Global Justice RMS and Global Computer Aided Dispatch requires the client, an authorized device, an authorized user, and has a user authentication system. Access to Global Justice RMS and Global CAD outside of the physically secure perimeter of the police department requires a two factor authentication consistent with CJIS security requirements. User access and authority is further restricted by user role or specific user rights established by the system administrator. Specific records can be further restricted to be accessed only by specified users. Police employees are the exclusive users of the RMS and CAD. Department personnel, and those who have responsibility to configure and maintain computer systems, networks, CAD and RMS, must successfully pass a

thorough background screening, including state and national criminal history records checks by fingerprint identification.

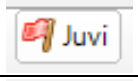
Person Identification Numbers

A unique and permanent seven digit Person ID Number is automatically generated for every person in the alphabetical RMS Master Name Index (MNI). "Involvements" (arrests, citations, incidents, contacts, vehicles, associates, etc.) for a person are linked to that person using the person ID. Identifying and contact information, and involvement history are available in the person's MNI file and Person Detail Report. Before a new person is created in RMS, RMS MNI is searched to determine if there is an existing match in the system. OP.55.66 establishes criteria for matching and merging RMS records.

Identification and Separation of Juvenile Records

Records of juveniles shall be kept separate from records of adults (938.396 and 48.396).

Person records are stored electronically by unique person ID number in the department's Global Justice RMS. The RMS specifically identifies juvenile records to prevent unauthorized access and release. RMS Master Name Index, Incident, Citation, Arrest, Accident, and Police Report records of juveniles are identified as such and automatically red flagged or marked. Legacy paper mug shots of juveniles are kept in separate binders. The department does not maintain fingerprint files.

MNI	
Incident	
Accident	
Citation	
Arrest	
Police Report Person	**"Juvenile"**

Use of Information Derived Solely from DOT Records

Since 2012, and since the U.S. Court of Appeals for the Seventh Circuit ruled that police re-disclosure of certain information derived from motor vehicle records is prohibited unless disclosed under an exception to the Driver's Privacy Protection Act, there has been much confusion and controversy for law enforcement agencies of what personal information can be released when gleaned from a DOT record. On May 10, 2016, the Wisconsin Court of Appeals issued its decision in *New Richmond News v. City of New Richmond* and provided some direction to law enforcement agencies for responding to public records requests for law enforcement

accident reports and incident reports that contain "personal information" and "highly restricted personal information" from department of motor vehicle records.

Three core principles emanate from the Court of Appeals' May 10, 2016 decision:

Uniform Traffic Accident Reports

Law enforcement agencies can release unredacted uniform traffic accident reports in response to a public records request even if personal information in the accident report came from a DMV record. The Court of Appeals found a DPPA exception permitting public access to this information applied which allows disclosure of personal information if specifically authorized under state law where such use is related to the operation of a motor vehicle or public safety. The Court of Appeals concluded that Wis. Stat. § 346.70(4)(f) specifically authorizes public access to accident reports, such that law enforcement agencies can provide unredacted copies of accident reports without violating the DPPA.

Incident Reports

With regard to incident reports, the Court of Appeals found the DPPA prohibits the release of personal information from a DMV record unless a specific exception in the DPPA allows release. The DPPA only permits release of personal information if one of fourteen narrow exceptions applies, and highly restricted personal information may only be released if one of four narrow exceptions applies. Although the DPPA provides an exception for a government agency to release personal information in a DMV record in carrying out its "functions," the Court concluded that responding to a public records request was not a "function" within the meaning of the DPPA exception.

Information Verified Using DMV Records

The Court of Appeals found that if personal information was first obtained from other sources and was only verified using DMV records, then that personal information is not prohibited from release by the DPPA.

The Wisconsin Court of Appeals ruling will have minimal impact on the operations of the Middleton Police Department as the department has been following similar guidelines since 2012. As in the past, officers should continue to seek other sources to verify personal information which is obtained from the Department of Transportation and which will be incorporated into department records; specifically information which will be used in an incident report.

If DOT is to be the sole source for personal information that is to be incorporated in department records, the officer shall notify the Records Bureau of the incident number and what the sole source personal information is (DL #, Address, VIN, DOB) so that personal information can be redacted before disclosure to non-excepted third parties. The Records Bureau will place a “Watch” on the record which will notify employees who access or view the record that the

record is DPPA restricted, and what the sole source DOT information is. If a redacted version of the document is produced, it may be saved in the document tab for the incident for future use.

Personal information derived solely from the Department of Transportation shall not be disclosed or made available to non-excepted third parties. There are 14 specific exceptions. The relevant exceptions are:

1. For use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls or advisories;
2. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private persons or entity action on behalf of a federal, state, or local agency in carrying out its functions;
3. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court;
4. For any other use specifically authorized under the laws of the state that holds the records, if such use is related to the operation of a motor vehicle or public safety; and
5. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, anti-fraud activities, rating or underwriting.

Criminal Identification Records

Collection

As required by 165.84(1), the department will obtain fingerprints and photographs, and other available identifying data, for adults and juveniles arrested or taken into custody for an offense of a type designated in s. 165.83(2)(a), if that person will not be "booked" at the Dane County Jail.

1. For an offense which is a felony or which would be a felony if committed by an adult.
2. For an offense which is a misdemeanor, which would be a misdemeanor if committed by an adult or which is a violation of an ordinance, and the offense involves burglary tools, commercial gambling, dealing in gambling devices, contributing to the delinquency of a child, dealing in stolen property, controlled substances or controlled substance analogs under ch. 961, firearms, dangerous weapons, explosives, pandering, prostitution, sex offenses where children are victims, stalking, harassment, or worthless checks.
3. For an offense charged or alleged as disorderly conduct but which relates to an act connected with one or more of the offenses under subd. 2.
4. Persons arrested or taken into custody as fugitives from justice (capias, warrant).

If fingerprints and/or a current photo are not in the system for a child taken into custody as a run away from his or her parents, guardian or legal or physical custodian, fingerprints and/or a current photo should be obtained.

At their discretion, officers may obtain fingerprints and photographs and other available identifying data of persons arrested or taken into custody for offenses other than those designated s. 165.83(2)(a).

Live Scan Fingerprint Procedure

State Charges – Juveniles and Adults:

1. Transmit prints electronically
    a. There is no need to print any cards

Municipal Charges – Adults

1. Transmit prints electronically
    a. There is no need to print a ten print card
2. Print a Disposition Card DJ-LE-249 (four finger slap)
    a. Submit the Disposition Card with report

Municipal Charges – Juvenile

1. Transmit prints electronically
    a. There is no need to print a ten print card
2. Do not print Disposition Card DJ-LE-249 (four finger slap), unless charging a 16-year-old with a traffic offense
    a. CIB will not accept juvenile fingerprint disposition cards for criminal or ordinance violations.

Juvenile Runaways – Wis. Stats. §48.19(1)(d)4

1. Transmit prints electronically
2. Do not print a fingerprint card
3. MIPD records does not maintain any fingerprint records

Retention and Storage

Fingerprints are obtained by live scan and are sent electronically directly to the Crime Information Bureau (TCN's and ATN's are automatically generated by the live scan device). The department does not maintain fingerprint record files. Identification photos are stored in the RMS Master Name Index (MNI) image section for the specific person. The RMS specifically identifies juvenile records to prevent unauthorized access and release. MNI records of juveniles are identified as such and automatically red flagged or marked (supra). Legacy paper mug shots of juveniles are kept in separate binders. Any person arrested or taken into custody and subsequently released without charge, or cleared of the offense through court proceedings, shall have any fingerprints or identification photos taken in connection therewith returned upon request [165.84(1)].

Release of Juvenile Identification Records

Dissemination of juvenile identification records is restricted to the confidential exchange of information between law enforcement agencies.

Warrant and Wanted Person Files

It is the policy of the department to establish a system governing verification, entry, access to and cancellation of Municipal Court Warrants, Commitments, and Service Warrants, and Temporary Felony and Misdemeanor Warrants, and Probable Cause to Arrest Files.

Warrant and wanted person records are stored in the Middleton Police Communications Center and are accessible by department personnel 24-hours a day.

All criminal misdemeanor and felony warrants are obtained through the District Attorney's Office and held, entered, and verified by the Dane County Sheriff's Office.

Municipal Warrants

The Crime Information Bureau (CIB) and National Crime Information Center (NCIC) computerized files via the TIME System are utilized as the medium to report warrants. The following procedure will be followed when entering and cancelling warrants in these systems.

1. The department must have in its possession a signed Municipal Court Warrant, Commitment, or Service Warrant.
2. A warrant file bearing the defendants name shall be created and filed alphabetically in the warrant file in the Communications Center.
3. Information emanating from department reports shall be verified for validity. The validity check and entry functions should be performed by different people or at different times.
4. The Warrant shall be entered into CIB/NCIC with a geographical pickup restriction of Dane and adjacent counties, except service warrants may be served anywhere in Wisconsin. Entry should be noted on the warrant file.
5. A DOJ Warrant Worksheet shall be completed and stored in the Warrant Worksheet Binder.
6. The warrant file shall contain the original warrant, supporting documents, CIB/NCIC entry printout, DOT return, and CIB/III Identification Data printouts.
7. Upon receipt of Hit Confirmation Request by the Communications Center, the Communications Center will furnish a substantive response of either positive or negative confirmation as to whether the record is active or not within ten minutes.
8. Entries in the CIB and NCIC files must be promptly canceled when the department learns the entry is no longer valid for whatever reason: apprehension of the wanted subject, withdrawal of the warrant, or expiration of the six-year retention period (from date of offense). A warrant need not be cancelled if a detainer is also entered for a subject known to be incarcerated in another jurisdiction.
9. When a warrant is cancelled, the warrant worksheet shall be pulled, updated and placed in the Warrant Folder along with a copy of the TIME system cancellation printout. The Warrant Folder shall be forwarded to the Municipal Court Clerk with appropriate notation.

Temporary Felony and Misdemeanor Warrants

The procedure for Temporary Warrants is the same as Municipal Warrants, except for the following:

1. Temporary Warrants must be approved by a Sergeant or above before entry.
2. In place of a warrant the department must have an investigative report sufficient to obtain a warrant, a probable cause affidavit, arrest document (SAC), booking sheet, and show that because of extenuating circumstances the department was unable to obtain the

warrant. (Examples of allowable circumstances could be the time of day, availability of the judge, etc.)

3. These warrants are entered into CIB/NCIC as temporary felony or temporary misdemeanor wants and retained in file for 48 and 72 hours respectfully. The geographic restriction may be adjusted as appropriate.
4. Entries in the CIB and NCIC files must be promptly canceled when the department learns the entry is no longer valid for whatever reason: apprehension of the wanted subject, withdrawal by the department, expiration of the retention period, or issuance of a warrant.
5. After cancellation, the Warrant Folder shall be forwarded to the Court Officer.

Probable Cause to Arrest Files

When there is probable cause to arrest a subject, the subject is at large, and a warrant will be requested if the subject is not apprehended, a special Probable Cause to Arrest File may be created to facilitate apprehension by other officers and booking.

1. Probable Cause to Arrest Files shall be stored alphabetically in the designated location in the Communications Center.
2. Red urgent handling document folders shall be utilized and contain the following:
    a. DOT return, and CIB/III Identification Data printouts, if any.
    b. Arrest Documents (SAC)
    c. Probable Cause Affidavit
    d. Booking Sheet
3. A briefing notice should be disseminated and updated upon withdrawal, apprehension, or issuance of a warrant. PC to arrest information presented at briefings or in briefing notices should be verified with the Communications Center before acted on.
4. Probable Cause to Arrest Files shall be promptly removed from the Communications Center upon withdrawal, apprehension or issuance of a warrant. The PC Affidavit and booking sheet should be utilized if the subject is to be booked at the Dane County Jail. The file should be forward through the Records Bureau to the Court Officer.

Information from Other Jurisdictions

The department shall not accept or enter warrants from other jurisdictions. Information received from other jurisdictions relating to warrants and wanted persons is relayed to department personnel through shift briefings and briefing notices. Briefing information should be updated if or when new information is received. Nonetheless, this information should always be verified before it is acted on.

Personnel Records

Purpose

Supervisory and management decisions must be based on the best information available. Therefore, accurate and up to date information must be maintained on all department personnel. Because of the contents, use, and access to these records varies, this order prescribes the nature of these various records, responsibility for maintaining them, and the rules relating to their security.

Department Roster (and emergency information)

The Office Manager shall periodically publish a department roster showing current addresses and telephone numbers of all department personnel and giving their date of employment with the department.

Emergency information shall be maintained in electronic files maintained by the Office Manager and on the employee's annual service record, which is held in the employee's Service File in the secure supervisor equipment room. In addition to name, address, and telephone number, this information shall include the name, relationship and telephone number of persons to contact in case of emergencies and the name and telephone number of the employee's health care provider.

Supervisors shall collect and update this information at least annually. Employees shall notify their supervisor and the Office Manager of any changes.

Service Files, Annual Service Records

Service files are working paper and electronic files maintained by supervisors and are built around an "annual service record." The annual service record is a record of current employee information and a chronological record of duty assignments, annual qualifications, discipline and commendations. The supervisors' working notes may be kept in these files.

Normally, the contents of a service file should not be forwarded to the employee's personnel file. However, the contents should be summarized in the employee's annual performance assessment report (evaluation). Documents or entries made in an employee's service file, other than changes to emergency contact information, shall be maintained in the service file for at least 12 months or as long as the employee's supervisor deems them pertinent, whichever is longer. All regular performance assessments (evaluations) will become part of an employee's permanent personnel file.

Personnel File

Personnel Files are maintained by the Office Manager and are to be kept in the secure administrative records room and shall be maintained indefinitely. Personnel files are the formal permanent record of an individual's employment history. They contain applications, letters of appointment, relevant correspondence, personnel orders, evaluations, and any other material which the Chief deems relevant, excluding material related to pre-employment background investigations and protected health information.

Any employee may inspect their personnel file and challenge the relevancy or accuracy of any information contained therein. Such inspection shall be with the prior approval of the Chief, during normal working hours and under the supervision of the Office Manager or designee.

Training File

Training Files are maintained by the Office Manager and training coordinator and may be paper, electronic or both. Training files are the formal permanent record of an employee's training including academy, initial or field, in-service, specialized, remedial, and academic training, and certificates, licenses, permits, and diplomas. Field Training records may be stored in an alternate

location at the discretion of the training coordinator, after the employee has been granted permanent status.

Release of Records

Requests for operational police records (records related to police incidents, calls for service, and the like) will normally be received or referred to the Records Bureau or Records Custodian who will conduct an analysis to determine if the record can be disclosed or partially disclosed after considering open records laws (State & City) and the department's Open Records policy.

Requests for administrative records (personnel, complaints, financial, payroll, etc.) will normally be received or referred to the Office Manager or Records Custodian who will conduct an analysis to determine if the record can be disclosed or partially disclosed after considering open records laws (State & City) and the department's Open Records policy.

Under no circumstances shall police records from another police agency be released by members of the department without prior permission from the police agency who has authority over these records.

In circumstances different from those stated above, police employees shall not release or disseminate any police record without the consent of a member of the police command staff with the following exceptions:

1. Use or disclosure of the record is necessary to carry out a department function or investigation.
2. The record has already been analyzed by the Records Bureau or Records Custodian and made available for pickup by or delivery to the requestor.
3. The confidential exchange of information between Law enforcement agencies, DCHS, DOJ, DOC, DA, CA, Department of Health and Family Services, and if requested by a fire investigator to pursue an investigation under 165.55.
4. Disclosure by a School Liaison Officer to an official of the school attended by a juvenile, or the district administrator or designee, of records relating to the use, possession, or distribution of alcohol or a controlled substance, illegal possession by a juvenile of a dangerous weapon; an act for which a juvenile was taken into custody under s. 938.19 based on a law enforcement officer's belief that the juvenile was committing or had committed a violation of any state or federal criminal law, or for an act for which a juvenile was adjudged delinquent [938.398(1)(b)(2) & 938.398(1)(c)(3)].

Destruction of Records

The retention periods for public records maintained by the Police Department vary and are delineated within the respective policies governing each type of record. The eventual destruction of public records held by the Police Department shall be conducted in accordance with City of Middleton Ordinance 2.23(7).