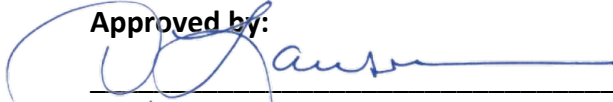
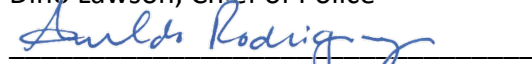


REPORT TO CITY COUNCIL

Approved by:



Dino Lawson, Chief of Police



Arnoldo Rodriguez, City Manager

Council Meeting of: January 18, 2023

Agenda Number: B-8

SUBJECT:

Access to The Superior Court of California, County of Madera Web-Based Portal

RECOMMENDATION:

Adopt a Resolution approving an Agreement between The Superior Court of California, the County of Madera, and the City for access to the Justice Partner Portal

SUMMARY:

The Superior Court of California, County of Madera (Court) launched a web-based portal, the Justice Partner Portal (JPP), for police departments to access restricted case information and other documents. Staff is seeking to enter a usage agreement with the Court to access the JPP. The Court will make the program available at no cost to the City.

DISCUSSION:

Police work requires an enormous amount of information sourcing from various parties. The Court is utilized as a primary source for gathering information on individuals due to its ability to keep records the City cannot legally maintain. The Court launched a web-based portal for agencies to access restricted case-related documents quickly and accurately. Providing City officers access to the JPP will enhance service delivery as the department will have secure and rapid access to vital information to better protect and serve the community. It is recommended that the City enter the usage agreement permitting access to the JPP.

It should be noted that the usage agreement would become effective January 18, 2023, and has no termination date unless either party chooses to pursue severance.

FINANCIAL IMPACT:

Use of the JPP will have no financial impact on the City as the Court is not assessing any fees for accessing the portal.

ALTERNATIVES:

Council may choose to deny entering the usage agreement or may request staff return with additional information.

ATTACHMENTS:

1. Resolution Approving Usage Agreement
2. Justice Partner Portal Usage Agreement

RESOLUTION NO. 23-_____

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF MADERA
APPROVING A USAGE AGREEMENT BETWEEN THE SUPERIOR COURT OF
CALIFORNIA, COUNTY OF MADERA, AND THE CITY FOR ACCESS TO THE
JUSTICE PARTNER PORTAL**

WHEREAS, The Superior Court of California, County of Madera (Court), launched a web-based portal, the Justice Partner Portal (JPP), for police agencies to access restricted case documents; and

WHEREAS, The City of Madera (City) utilizes case information from the Court and would benefit from access to the portal; and

WHEREAS, The City is seeking access to the JPP to aid in efforts to better serve and protect the community; and

WHEREAS, the usage agreement becomes effective January 18, 2023, and has no termination date; and

NOW, THEREFORE, THE COUNCIL OF THE CITY OF MADERA hereby resolves, finds, determines, and orders as follows:

1. The above recitals are true and correct.
2. The Usage Agreement between the Superior Court of California, Madera County, and the City of Madera for access to the Justice Partner Portal, a copy of which is attached hereto as Exhibit 1, is approved.
3. The Chief of Police is authorized to electronically execute all necessary documents required to enter the agreement.
4. This resolution is effective immediately upon adoption.

* * * * *



**SUPERIOR COURT OF CALIFORNIA
COUNTY OF MADERA**

**Justice Partner Portal Usage Agreement
Between
The Superior Court of California, County of Madera
and
The City of Madera**

January 18, 2023

Madera Superior Court Justice Partner Portal Usage Agreement

1. Introduction

This Usage Agreement ("UA") is entered into by and between the Superior Court of California, County of Madera ("Court") and the City of Madera ("Agency"), each a "Party" and collectively, the "Parties." This Agreement is effective on January 18, 2023 ("Effective Date").

1.1 Purpose

The Justice Partner Portal (JPP) provides authorized agencies access to restricted case information and documents through a secure website.

1.2 Scope

This policy governs connectivity to the court's case management system via the JPP.

This policy should be supplemented by governing business policies for specific application access, if applicable.

The technical requirements and limitations placed on an entity connecting to the court from any network are dependent on the application utilized to access the JPP and its associated business policy and the type of remote user and workstation used for access (including laptops or other mobile devices).

1.3 Audience

This policy is written for justice partners who require JPP access.

2. Term

The term of this MOU shall begin on the Effective Date noted above and shall continue to be in effect until terminated by either Party in accordance with section 11 of this UA.

3. Court Data

- 3.1 "Court Data" means the electronic records as set forth in the California Rules of Court, Title 2, Division 4, Chapter 2, Article 4.
- 3.2 The Agency acknowledges that Court Data may include: (i) data and information that is designated as confidential, or that the Agency otherwise knows, or would reasonably be expected to know is confidential; (ii) personally-identifiable information (e.g., person's name, address, driver's license number, credit card number, social security number, email address, etc); (iii) medical and health data; (iv) law enforcement records; and (v) passwords, security codes, or similar access control information.
- 3.3 Notwithstanding any provision to the contrary, Court Data may only be used by the Agency for its own internal use for the sole purpose of performing its statutory duties. Agency may not disclose Court Data to any third parties.
- 3.4 The Agency represents and warrants that any access by the Agency to Court Data shall be in compliance with applicable laws. Agency will indemnify, defend, and hold harmless the Court and its personnel from all claims, liability, damages, and expenses arising out of the Agency's breach of the

foregoing representation and warranty. Agency's access to and use of Court Data shall be governed by all applicable privacy laws, statutes, rules, and regulations.

4. Access

- 4.1 Maintenance windows of the JPP shall be exclusively determined by the Court and/or the Court's contracted vendor of the JPP.
- 4.2 Remote Support Access for Justice Partners: JPP access issue assistance requiring court resources is available during court business hours.
- 4.3 The JPP access for the Agency is limited to the specific electronic records identified under California Rule of Court 2.540(b) that are authorized for the specific Agency.
- 4.4 Should the Agency wish to request expanded access, they must file a written request identifying good cause as noted in California Rule of Court 2.540(b)(1)(Q) for consideration by the Presiding Judge or his/her designee. All such written requests for expanded access must be submitted to Court Administration (Amy Downey: amy.downey@madera.courts.ca.gov), who will notify the Agency of the outcome of the requests.
- 4.5 The Court will control access by enabling and disabling User IDs on an as-needed-basis only. Access will not be granted until the identity of the user has been verified in a method determined by the Court, and as specified by Rule 2.541 of the California Rules of Court.
- 4.6 Should a new employee require access, the Agency is to request the Court to create a user profile for the individual using the form attached herein as Exhibit A.
- 4.7 Should an employee leave their position with the Agency, it is the responsibility of the Agency to notify the Court immediately so access may be terminated.
- 4.8 All users of the JPP, or any other database that contains non-criminal history information, agree, as a condition to being provided access to the JPP or any other database, that they shall not access or use any information contained within the JPP or any other database for immigration enforcement purposes, except that the users are not restricted in the use of criminal history information and are not restricted in the use of information regarding a person's immigration or citizenship status pursuant to 8 USC sections 1373 and 1644.

5. Confidentiality

- 5.1 Notwithstanding any provision to the contrary, during the term of this UA and at all times thereafter, Agency will: (i) hold all Court Data in strict trust and confidence, (ii) refrain from using Court Data in any manner or for any purpose not expressly permitted by this UA, and (iii) refrain from disclosing or knowingly permitting others to disclose or use any Court Data, except if Agency is required to disclose Court Data to comply with Data Recipient's statutory obligations.
- 5.2 Agency will disclose Court Data only to its employees with a legitimate need to know in order to use the data for Data Recipient's internal use solely to perform the Data Recipient's specific statutory duties.
- 5.3 Agency agrees to advise employees who are authorized to access Court Data that pursuant to Penal Code sections 13302 and 13303, any person who knowingly furnishes information other than as authorized by law is guilty of a misdemeanor.

- 5.4 Agency will protect Court Data from unauthorized use, access, or disclosure in the same manner as Agency protects its own confidential or proprietary information of a similar nature, and with no less than reasonable care and industry-standard care.
- 5.5 Upon the Court's request, or upon any termination or expiration of this UA, Agency shall certify to the Court in writing within five (5) business days that Agency has fully destroyed Court Data in a manner that is unrecoverable and in accordance with highest and leading industry-standards regarding data destruction, including administrative, physical, technical, and procedural safeguards..
- 5.6 Agency acknowledges that there can be no adequate remedy at law for any breach of Data Recipient's obligations hereunder, that any such breach will likely result in irreparable harm, and therefore, upon any breach or threatened breach of the confidentiality obligations, the Court shall be entitled to appropriate equitable relief, without the requirement of posting a bond, in addition to its other remedies at law.

6. Data Security

- 6.1 Agency shall comply with and implement Data Safeguards. "Data Safeguards" means the highest industry-standard safeguards (including administrative, physical, technical, and procedural safeguards) against the destruction, loss, misuse, unauthorized disclosure, or alteration of the Court Data, and such other related safeguards that are set forth in applicable laws, or pursuant to the Court's policies or procedures or as required by judicial order.

To the extent that Agency has internal policies or procedures currently in place, such policies or procedures may be utilized to fulfill obligations for Data Safeguards. Data Safeguards employed by the Agency are subject to review and audit by the Court to determine compliance with this UA. If the Court finds Agency's Data Safeguards to be lacking or deficient, Agency shall have thirty (30) days to remedy deficient Data Safeguards. If the Court provides the Agency with electronic access to data, any assigned user ID or established password may not be shared with or used by any other person. The Court may monitor Data Recipient's access at any time, with or without notice, for the purpose of ensuring compliance with this UA.

- 6.2 Agency may not store or transmit Court Data outside the continental United States. When accessing Court Data, Agency may not access it from outside the continental United States. The physical location of Agency's data center, systems, files, and equipment where Court Data is stored shall be within the continental United States.
- 6.3 Connections to Agency's computers or other electronic devices utilizing the Internet must be protected using at least one of the following industry standard cryptographic technologies such as SSL VPN, IP-Sec VPN or OPEN VPN. Each client workstation, including laptops and other mobile devices, must be the property of the court or Agency. Access from home is not allowed unless utilizing equipment approved by the Agency to be compliant and accessed through secure VPN access as noted above. Agency shall not access Court Data from public computers. Agency workstations must be governed by a security/management policy requiring virus protection and security patches.

Regardless of the media employed (i.e., disk, tape, etc.), Court Data must be stored in an encrypted format.

- 6.4 Agency shall provide periodic training for staff on Agency internal security policies and procedures, and on applicable state and federal legal requirements for protecting data, including sensitive, confidential, and personal data.
- 6.5 Agency shall certify that all staff members with access to Court Data have been subjected to a bona fide criminal background check and have no record of any felony convictions. Any exceptions to this requirement must be approved in writing by the Court. Background checks shall be conducted by a local law enforcement agency using LiveScan fingerprinting. Background checks shall include DOJ, FBI, and Local checks.
- 6.6 Agency shall promptly notify the Court upon receipt of any requests that in any way might reasonably require access to Court Data. Agency shall not respond to subpoenas, service of process, Public Records Act requests (or requests under California Rule of Court 10.500), and/or other legal requests directed at Agency regarding this UA or Court Data without first notifying the Court. Except as prohibited by applicable law, Agency shall provide its intended responses to the Court with adequate time for the Court to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Agency shall not respond to legal requests directed at the Court unless authorized in writing to do so by the Court. Notwithstanding the foregoing or any applicable law regarding public records, Agency shall comply with all applicable laws regarding the confidentiality of Court Data.

7. Compliance with Applicable Laws

Agency shall comply with all applicable laws, rules, and regulations, including without limitation, privacy and data protection laws, and California Rules of Court that govern the Court Data. Agency shall also comply with all privacy and data security requirements set forth in the Court's policies and procedures. Agency certifies that its network is and shall continue to be operated in compliance with all relevant federal and state laws, regulations, rules, and policies.

8. Data Breaches

- 8.1 If there is a suspected or actual Data Breach, Agency shall notify the Court in writing within forty-eight (48) hours of becoming aware of such occurrence.

Court Contact: Daniel Smith (559) 517-7085 (Daniel.Smith@madera.courts.ca.gov)

A "Data Breach" means any access, destruction, loss, theft, use, modification or disclosure of Court Data by an unauthorized party, or any unauthorized use of a Court-provided user ID or password. Data Recipient's notification shall identify: (i) the nature of the Data Breach, (ii) the data accessed, used or disclosed; (iii) who accessed, used, disclosed and/or received the Court Data (if known); (iv) what Agency has done or will do to mitigate the Data Breach; and (v) corrective action Agency has taken or will take to prevent future Data Breaches.

- 8.2 Agency shall promptly investigate the Data Breach and shall provide weekly updates, or more frequently if required by the Court, regarding findings and actions performed by Agency until the Data Breach has been resolved to the Court's satisfaction, and Agency has taken measures satisfactory to the Court to prevent future Data Breaches. Agency bears sole responsibility for notifying the affected person(s) as or if required by Civil Code section 1798.29. Agency shall conduct an investigation of the Data Breach and shall share the report of the investigation with the Court. The Court and/or its authorized agents shall have the right to lead or participate in the investigation. Agency shall cooperate fully with the Court, its agents and law enforcement, including with respect to

taking steps to mitigate any adverse impact or harm arising from the Data Breach. Agency shall comply with all applicable laws regarding data breach notification.

- 8.3 After any Data Breach, the Court, at its option and own cost, may have an independent, industry-recognized, Court-approved third party perform an information security audit. Upon Agency receiving the results of the audit, Agency shall provide the Court with written evidence of planned remediation within thirty (30) calendar days and promptly modify its security measures in order to meet its obligations under this UA.

9. Disclaimers

THE COURT DATA IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. THE JUDICIAL BRANCH ENTITIES DO NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING, AND SHALL NOT HAVE ANY LIABILITY REGARDING, THE ACCURACY, RELIABILITY, COMPLETENESS, OR AVAILABILITY OF COURT DATA, AND ARE NOT RESPONSIBLE FOR ANY DISCREPANCIES BETWEEN COURT DATA AND DATA FROM OTHER SOURCES, INCLUDING ANY OFFICIAL RECORD. IN NO EVENT SHALL THE JUDICIAL BRANCH ENTITIES BE LIABLE FOR CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES. "Judicial Branch Entities" shall mean the Court and any California superior or appellate court, the Judicial Council of California, and the Habeas Corpus Resource Center. Under California Rule of Court 2.504(b), unless electronically certified by the court, a trial court record available by electronic access is not the official record of the court.

10. Indemnification

Agency shall indemnify, defend, and hold harmless the Judicial Branch Entities (and their officers, employees, agents, and contractors) from and against all liabilities, damages, claims, losses, and expenses arising out of Data Recipient's (or its directors, officers, employees, agents, or contractors) acts, omissions, or breach of this UA or its access, use, storage, or disclosure of Court Data, as well as noncompliance with applicable laws, rules, and regulations.

11. Termination

- 11.1 Provided that it gives the other Party at least thirty (30) days prior written notice, either Party may terminate this UA with or without cause. In addition, any violation of the terms in this UA by Agency may result in the immediate termination of JPP access for the entire department. The Agency agrees that remote access to electronic records under California Rules of Court, Title 2, Article 4 is a privilege and not a right. The Court reserves the right to immediately suspend data access to the Agency, without prior notice (if prior notice is not feasible): (i) if the Court determines that there has been a breach by Agency under this UA; or (ii) if the Court determines, in its sole discretion, that such suspension is necessary to protect its data, systems, Court personnel, Judicial Branch Entities, or the public. In all circumstances, the Agency will ultimately be notified of any data access suspension.
- 11.2 Upon the expiration or termination of this UA, Agency shall certify in writing within five (5) business days that all copies of the Court Data stored on Agency servers, backup servers, backup media, or other media (including paper copies) have been permanently erased or destroyed. "Permanently erased" means the data have been completely overwritten and are unrecoverable.
- 11.3 Sections 9 through 13 of this UA shall survive the termination or expiration of this UA.

12. Notices

Except as otherwise specifically set forth in this UA, any notice required or permitted under the terms of this UA or required by law must be in writing and must be: (i) delivered in person, (ii) sent by registered or certified mail, or (iii) sent by electronic mail, in each case properly posted and fully prepaid to the appropriate address and recipient set forth below:

If to the Agency:
City of Madera

Attn: Chief of Police
330 South C Street
Madera, CA 93638

If to the Court:

Superior Court of California, County of
Madera
Attn: Chief Financial Officer
200 South G Street
Madera, CA 93637

Either Party may change its address for notification purposes by giving the other Party written notice of the new address in accordance with this Section. Notices will be considered to have been given at the time of actual delivery in person, three (3) business days after deposit in the mail as set forth above, or one (1) day after delivery via electronic mail.

13. Miscellaneous

- 13.1 Agency may not assign, subcontract, delegate, or otherwise transfer its rights, duties, or obligations under this UA without the prior written consent of the Court.
- 13.2 The Parties waive the per capita risk allocation set forth in Government Code section 895.6. Instead, the Parties agree that if one of them is held liable upon any judgment for damages caused by a negligent or wrongful act or omission occurring in the performance of this UA, the Parties' respective pro-rata shares in satisfaction of the judgment will be determined by applying principles of comparative fault.
- 13.3 Each Party represents and warrants that it has full power and authority to enter into this UA, and that its representative who signs this UA has the authority to bind such Party to this UA. Any waiver or failure to enforce any provision of this UA on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion. If any part of this UA is held unenforceable, all other parts remain enforceable. The Parties shall attempt in good faith to resolve informally and promptly any dispute that arises under this UA. This UA shall be governed by the laws of the State of California, without regard to its conflict of law provisions.
- 13.4 This UA, including its exhibits and attachments, contains the entire and complete understanding of the parties hereto and supersedes any and all other previous or contemporaneous agreements, representations, and warranties, whether oral or written. Court and Agency may amend this UA by mutual consent, in writing, at any time. References to and mentions of the word "including" means "including, without limitation." Section headings are for reference and convenience only and shall not be considered in the interpretation of this UA.

The Superior Court of California, County of Madera
Justice Partner Portal Acceptable Use Policy

Superior Court of California,
County of Madera

City of Madera

BY: _____
(Authorized Signature)

BY: _____
(Authorized Signature)

Adrienne Calip

(Printed Name)

Dino Lawson

(Printed Name)

Court Executive Officer

(Title)

Chief of Police

(Title)

(Date)

(Date)

EXHIBIT A

JUSTICE PARTNER PORTAL ACCESS REQUEST FORM

Once this form is complete and signed,
please scan and e-mail it to the Portal
Administrator at portaladmin@madera.courts.ca.gov

SUPERIOR COURT OF CALIFORNIA • COUNTY OF MADERA

JUSTICE PARTNER PORTAL ACCESS REQUEST FORM

Agency Name or Law Firm Name: _____

Date Requested: _____

	Request Type	First Name	Last Name	Email Address	Role
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					

By signing this agreement, I confirm my understanding that access to electronic records via the Justice Partner Portal ("Portal") is subject to the terms and conditions of the Justice Partner Portal Acceptable Use Policy ("Policy"). I certify that I have advised all employees noted above that pursuant to Penal Code Sections 13302 and 13303, any person who knowingly furnishes information other than as authorized by law is guilty of a misdemeanor. Our agency will only access the Portal for work-related purposes, and the Court may suspend or terminate my access pursuant to the provisions outlined in Section 11 of the Policy.

Agency Chief, Attorney, or Designee Name (Print)

Agency Chief, Attorney, or Designee Email Address

Date: _____

Agency Chief, Attorney, or Designee Signature

Phone Number to Verify