



## California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Notice for Employees

Your privacy is very important to Mission Federal Credit Union (“Mission Fed”). The California Consumer Privacy Act (/California Consumer Privacy Rights Act (“CCPA/CPRA”) requires Mission Fed (collectively, “we”, “us” or “our”) to provide additional information to California residents, including Mission Fed employees (“employees”), about the ways in which we collect, retain, process, and share your personal information. This notice shows the types of personal information we may collect from employees, the sources that provide the information we collect, and the ways in which we use and disclose it for both normal business purposes as well as in the event of a response to the novel coronavirus (“COVID-19”).

### **PERSONAL INFORMATION**

#### Categories of Personal Information

<b>General Categories</b>	<b>Examples</b>
<i>Personal Identifiers</i>	Real name, alias, postal address, unique personal identifier, online identifier, photo, internet protocol address, email address, account name, social security number, driver’s license or state identification card number, passport number, signature, physical characteristics or description, telephone number, insurance policy number, employment history, bank account number, credit or debit card number, medical information, health insurance information, financial information, immigration status, or other similar identifiers.
<i>Characteristics of Protected Classifications Under California or Federal Law</i>	Date of birth; age; gender; military or veteran status; marital status; nationality; citizenship; request for family care leave, pregnancy leave and leave for an employee’s own serious health condition.
<i>Biometric Information</i>	Physiological characteristics, including imagery of the iris, retina, fingerprint, face, hand, palm, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted.
<i>Internet or Other Electronic Network Activity</i>	Browsing history or information during interactions while on the Mission Fed network.
<i>Geolocation Data</i>	Geographical location derived from electronic devices, servers, or other similar devices.
<i>Sensory Data</i>	Audio, electronic, visual, or similar information.
<i>Education, Professional, or Employment Information</i>	Job titles, references, any employment information, details of your education history, degrees, and certifications.
<i>Inferences</i>	Any information identified to create a profile reflecting an employee’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

<b>COVID-19 Categories</b>	
<i>Medical and Health Data</i>	Measuring body temperature, screening questions regarding symptoms of COVID-19, and whether you have been tested for COVID-19.
<i>Close Contact Information</i>	Whether you have been in close contact with an individual who has tested positive for COVID-19 or has COVID-19 symptoms.
<i>Travel Information</i>	Whether you have recently traveled to a restricted or high-risk location; engaged in any activity that is considered high-risk including, but not limited to, concerts, bars, casinos, or any other place or event with large groups of people; gatherings where social distancing and/or the use of face cloth coverings were not practiced; and the dates you were in those locations.
<i>Other</i>	Responses to screening questionnaires, test results, and any other information you provide in connection with our health and safety measures.

Sources of Personal Information

We obtain the categories of personal information listed above from the following categories of sources:

- Information that you directly provide to Mission Fed (ex. Information for payroll or benefits);
- Information that you choose to make public (ex. Publicly visible social media profiles);
- Information from third parties who provide it to Mission Fed (ex. Background check agencies, government agencies, and law enforcement authorities); and
- Information collected through the Mission Fed Network (ex. Device type, browser type, browser settings, IP address, pages browsed, or other information).
- Information that you provide directly to Mission Fed in connection with our health and safety measures in response to COVID-19 or similar outbreaks.

How and Why We Use Your Personal information from Applicants

We may use or disclose the personal information we collect for any of the following purposes:

- *Business, Employment, and Human Resource Operations:* to support our everyday business operations including compensation activities, business continuity, managing and operating facilities, and to administer and maintain benefits and retirement plans;
- *Operation of Websites:* management of the Mission Fed website, intranet, and third-party Human Resources workforce management website including displaying information, communicating, and interacting with you;
- *IT Operations:* to conduct IT security audits, user identity and privileged management purposes, or other IT security related functions;
- *Security:* physical security of our branches and offices (including any video recordings or access logs) and electronic security (login records and access details).
- *Legal Matters:* to respond to law enforcement requests, court orders or other types of legal process including (subpoenas, levies, or garnishments);

- *Legal Compliance:* to comply with Mission Fed’s legal and regulatory obligations under applicable state and federal law;
- *Fraud and Risk Management:* to detect, evaluate and prevent fraud or in connection with audits, compliance reviews, exams, and other risk management functions;
- *Health and safety purposes:* to support health and safety measures that help reduce the risk of spreading and exposing individuals to COVID-19; identify employees and applicants who are displaying COVID-19 symptoms; communicate with employees and applicants who have tested positive for or are suspected of having COVID-19; and assist with contact tracing efforts in connection with COVID-19;
- *Recordkeeping:* your personal information is retained as required by law and in accordance with our record retention policies;
- *Legal Matters:* to respond to law enforcement requests, court orders or other types of legal process relating to COVID-19; and
- *Legal Compliance:* to comply with Mission Fed’s legal and regulatory obligations under applicable state and federal law relating to COVID-19.
- 

#### Third Parties that We Share Your Personal Information With

- Governmental, law enforcement, or regulatory authorities or agencies (when required to do so);
- Accountants, auditors, lawyers and other external professional advisors, subject to written agreements and confidentiality clauses;
- You and where appropriate, your family or your representatives;
- Third party service providers to support workforce management and Human Resource activities including administering and maintaining benefits and retirement plans;
- Other third parties to comply with legal requirements such as to respond to subpoenas and court orders or to address fraud, security, or technical issues;
- Third party service providers to support our health and safety measures such as providers of thermal body scanners; and
- Other third parties to comply with legal requirements relating to COVID-19.

#### Sale of Personal Information

Mission Fed does not sell personal information and has not done so in the past 12 months.

#### Request for More Information

For more information about our privacy practices, contact us at 1-858-546-2037 or email [humanresources@missionfed.com](mailto:humanresources@missionfed.com).