

California Employee Privacy Policy

Effective: January 1, 2023

Last Updated: August 23, 2024

What is the Purpose of this Document?

This California Employee Privacy Policy (the “Policy”) for San Joaquin Valley College, Inc. (“SJVCi”) and its divisions and subsidiaries, including, but not limited to, San Joaquin Valley College (SJVC), Ember Education, and Carrington College (collectively hereafter as “Employer,” “we,” or “our”), describes Employer’s processing of Personal Information from applicants, employees, and contractors. This Policy supplements any other privacy notices and is not intended to override them. This includes, but is not limited to, any provisions in the SJVCi Employee Handbook as it may be amended from time to time.

For the purposes of this Policy, “Personal Information” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to any individual or a household.

This Policy Describes

- Personal Information We Collect
- How We Collect Your Personal Information
- How We Use Your Personal Information
- How We Disclose Personal Information
- California Privacy Rights
- Changes to the Policy
- Questions About This Policy

Personal Information We Collect

Employer collects Personal Information about you during the application process and throughout the scope of your employment with Employer as well as when you fulfill a temporary contract position with Employer. The categories of Personal Information collected may include the following:

- **Identifiers**, such as your name, employee/staff ID, postal address, email address, date of birth, gender, nationality, and Social Security number or equivalent national identification number.
- **Family Information**, such as the name, relationship, date of birth, contact details, and social security numbers of your family members, marital status, and any other information that may be needed for the administration of benefits and to identify who to contact in the case of an emergency.

- **Information about your job**, such as job title, category and status, work location, department, employment contract, assigned tasks and projects, weekly hours, supervisor's name, start and end date, and reason for leaving.
- **Education Information**, such as your education and training background.
- **Internet and other electronic network activity information**, such as information technology systems usage information related to your use of Employer's equipment, systems, and other resources.
- **Audio and visual information**, such as video and call recordings.
- **Communication details**, such as email content, business letter content, business documents, and chat content.
- **Performance and disciplinary information**, such as performance reviews, evaluations and ratings, information about disciplinary allegations, the disciplinary process and any disciplinary warnings, details of grievances, and any outcome.
- **Information about your compensation and benefits**, such as your basic salary, bonus and commission entitlements, insurance benefits (including information about you and your dependents that we provide to the insurer), garnishments, hours and overtime, tax code, holiday entitlement, sick time, accrued salary information, and information relating to your retirement savings plan.
- **Professional or employment related information and documents**, such as professional certifications, prior work experience, employment agreements, confidentiality agreements, and proprietary rights agreements.
- **Financial information**, such as your bank details (for payroll and business expense reimbursement purposes only) and business travel and entertainment data.
- **Health information**, as required by law or as necessary to manage the employment relationship, including benefits administration, occupational health, disability accommodation, workers' compensation, and medical leave.
- **Characteristics of protected classifications under California or federal law**, such as race, color, sex/gender, marital status, national origin, disability, military or veteran information, request for leave for family care, health condition, or pregnancy, and age.
- **Termination and post-employment information**, such as termination agreements, benefits notices, and unemployment compensation forms.
- **Post-offer criminal background information**, such as any criminal history, revealing felony, misdemeanor, sex offender, probation, and other federal, state and county criminal offense records, as well as fingerprinting, Office of Inspector General (OIG) Sanctions List, General Services Administration's Excluded Parties Listed System, violent sex offender or predator registry search, applicable state exclusion lists, and U.S. Treasury Office of Foreign Assets Control (OFAC).

Sensitive Personal Information

We collect Personal Information that is defined as “Sensitive Personal Information” under California law, including driver’s license, social security numbers, race or ethnic origin, and health information. We use and disclose Sensitive Personal Information only as necessary: (i) to process your request for employment, (ii) provide services and benefits in connection with your employment, (iii) to comply with the law, and (iv) for business purposes reasonably expected within the scope of your employment.

Retention

For each of these categories of Personal Information, we will retain the information as long as is reasonably necessary to fulfill the purpose for which it was collected and to comply with applicable laws and regulations. We consider the following criteria when determining how long to retain Personal Information: why we collected the Personal Information, the nature of the Personal Information, the sensitivity of the Personal Information, our legal obligations related to the Personal Information, and the risks associated with retaining the Personal Information.

How We Collect Your Personal Information

We may collect your Personal Information from a variety of sources and methods. This includes:

Information You Voluntarily Provide to Us

We may collect Personal Information from you that you voluntarily provide to us as an applicant and during the scope of your employment or temporary assignment.

Information We Collect When You Use Our Systems

We collect Personal Information when you use our systems, including computer systems, security systems, time keeping systems, and any internal intranet or online platforms.

Information We Collect When You Use Our Website

Automated technologies or interactions. If you applied for a position through one of our websites, we receive and store internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data. When you access and use our website from your mobile devices, we receive data from that mobile device. This may include your device ID, location data, IP address and device type. You may manage how your mobile device and mobile browser share location information with us, as well as how your mobile browser handles cookies and related technologies by adjusting your mobile device privacy and security settings. Please refer to instructions provided by your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

Cookies. Our website may also place cookies on the device that you use to access the websites. Cookies are small files that we or our service providers transfer to your device through your web browser that enables us or our service providers’ systems to recognize your browser and capture

and remember certain information. We use cookies to help us understand how users use the website. For example, cookies gather information about how long you spend on a web page so that we can understand what web pages are of most interest to users. If you prefer, you can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off cookies by adjusting your browser settings. If you turn off your cookies, some of the features of the website may not function properly.

Your ‘Do Not Track’ Browser Setting. Some web browsers incorporate a “Do Not Track” feature (DNT) that signals to the websites that you visit that you do not want to have your online activity tracked. Many websites and applications, including ours do not currently respond to web browser DNT signals because such signals are not yet uniform. For more information about DNT signals, please visit <http://allaboutdnt.com>. Other third-party websites may keep track of your browsing activities when they provide you with content, which enables them to customize what they present to you on their websites.

Information We Collect From Third Parties

We collect Personal Information from service providers including where we operate accounts on third-party platforms, such as employee search and recruiting platforms, background check and employee eligibility providers, employee benefit providers, payroll providers, security providers, evaluation and training providers, support system platforms, curriculum platforms, emergency notification platform, electronic signature providers, and technology providers.

Google Analytics. We use third party cookies provided by Google Analytics to assist us in better understanding our website visitors. These cookies collect IP addresses and usage data, such as the length of time a user spends on a page, the pages a user visits, and the websites a user visits before and after visiting our website. Based on this information, Google Analytics compiles data about website traffic and interactions, which we use to offer better user experiences and tools in the future. For more information on Google Analytics, visit <https://support.google.com/analytics>.

Pixel Tags (aka clear gifs). Pixel tags are tiny graphics with a unique identifier that generally work in conjunction with cookies, which allow us to monitor the use of our Services. For example, we use pixels to count users who have visited website pages and for other related website statistics and to track advertising conversions and other tracking metrics. You cannot decline pixel tags; however, if you turn off or opt out of cookies the pixel tag will simply detect an anonymous visit.

How We Use Your Personal Information

Employer uses Personal Information, for all purposes related to your application for employment, administration of your temporary contract assignment, and the creation, administration, and termination of your employment or contractual relationship with the Employer and for all purposes related to Employer’s ongoing business operations. These purposes include, but are not limited to, the following:

- Making a decision about your recruitment or appointment.

- To assess your skills, qualifications, and suitability for the work or role for which you are applying.
- To carry out background and reference checks, where applicable.
- To communicate with you about the recruitment process.
- Determining the terms on which you work for Employer.
- Confirming you are legally entitled to work in the United States.
- To administer compensation, including, but not limited to, payment of wages and bonuses and income tax withholding and reimbursement of business expenses.
- Providing employment benefits to you if applicable, for example, medical insurance, dental insurance, vision insurance, life insurance, and retirement savings plans.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance, and determining performance requirements.
- Making decisions about salary and compensation levels.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of your working relationship with Employer.
- Education, training, and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your ability to perform the essential functions of your position with or without reasonable accommodation.
- To administer leaves of absence as required by law or company policy.
- Complying with health and safety obligations.
- To prevent fraud.

- To monitor your use of Employer’s information and communication systems to ensure compliance with Employer’s policies.
- To ensure network and information security, including preventing unauthorized access to Employer’s computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal employment opportunities and state fair wage laws monitoring.
- To exercise Employer’s rights under applicable law and to support any claim, defense, or declaration in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel.
- To meet legal and regulatory requirements including civil discovery in litigation involving Employer or affiliated companies.
- To apply for institutional and programmatic accreditations.
- To conduct clinical experiences at third-party affiliated sites.
- To confirm classroom attendance of students.
- To provide required directory information in course catalogs.
- To facilitate administrative functions, including, but not limited to, the management and operation of information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, strategic planning, and the maintenance of licenses, permits and authorizations applicable to Employer’s business operations.

How We Disclose Personal Information

Personal Information We Disclose for a Business Purpose

Information You Instruct Us to Share. You may be presented with an option to have us send certain information to third parties or give them access to it. If you choose to do so, your Personal Information and other information may be disclosed to such third parties and all information you disclose will be subject to the third-parties’ privacy policies and practices.

Service Providers. We may use third-party service providers to perform certain business services on our behalf and may disclose Personal Information to such service providers as needed for them to perform these business services. Service providers are only allowed to use, disclose, or retain the Personal Information to provide these services and are prohibited from selling Personal Information. Business services provided include, but are not limited to, employee search and

recruiting platforms, background check and employee eligibility providers, employee benefit providers, employee support fund administrator, payroll providers, security providers, evaluation and training providers, curriculum platforms, software subscriptions, accounting and audit services, compliance services, proctoring and testing services, support system platforms, emergency notification platform, electronic signature providers, and technology providers.

Internal Third Parties. We may share Personal Information with our parent company, subsidiaries and other companies owned by or controlled by Employer, who may use the Personal Information for the purposes described above.

Categories of Personal Information that have been disclosed for a business purpose in the past twelve months include:

- Identifiers
- Contact information
- Family information
- Information about your job
- Education information
- Internet and other electronic network activity information
- Audio and visual information
- Communication details
- Performance and disciplinary information
- Information about your compensation and benefits
- Professional or employment related information
- Financial information
- Health information
- Characteristics of protected classifications under California or federal law
- Termination and post-employment information
- Post-offer criminal background information
- Usage data

Personal Information Sold or Shared. We have not sold any Personal Information in the past twelve months. We have shared Personal Information in the past twelve months with our third party advertising partners to serve ads to you about our products and services as you browse the Internet. “Sharing” is defined under California privacy law as “renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s Personal Information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable

consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.” This sharing means that these third-party service providers may use their own cookies or tags to track your online activities and purchases in order to deliver targeted advertising based on your interests. You can opt of sharing through the [Do Not Share My Personal Information](#) link. Additionally, if your browser supports it, you can turn on the Global Privacy Control (GPC) to opt-out of the “sharing” of your Personal Information. Learn more at the [Global Privacy Control](#) website. We do not have any actual knowledge of selling or sharing Personal Information of minors under 16 years of age.

Business Transactions. We may do business with third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your Personal Information in the same way as set out in this Policy.

Legal Process. Subject to applicable law, we may disclose information about you (i) if we are required to do so by law, regulation or legal process, such as a subpoena; (ii) in response to requests by government entities, such as law enforcement authorities; (iii) when we believe disclosure is necessary or appropriate to prevent physical, financial or other harm, injury or loss; or (iv) in connection with an investigation of suspected or actual unlawful activity.

Information You Provide To A Third Party. Employer may contract with third party service providers that operate their own websites and online platforms on which you will need to create an account (“Third-Party Sites”). Employer does not control any Third-Party Sites and is not responsible for any information they may collect. The information collection practices of a Third-Party Site are governed by its privacy policy. It is your choice to enter any Third-Party Site. We recommend that you read its privacy policy if you choose to do so.

California Privacy Rights

California privacy law provides California residents with specific rights regarding their Personal Information. This section describes your privacy rights and explains how to exercise those rights.

Upon verification of your identity you may:

- No more than twice in any 12-month period, request disclosure of the following information:
 - Categories of Personal Information we collect.
 - Categories of sources from which Personal Information is collected.
 - Business or commercial purposes for collecting, selling or sharing Personal Information.
 - Categories of Personal Information sold or disclosed to third parties.

- Categories of third parties with whom such Personal Information is disclosed.
 - Specific pieces of Personal Information we collect.
- Request to correct inaccurate Personal Information.
 - Request deletion of your Personal Information, subject to the exceptions provided by law.
 - Opt-out from having your Personal Information sold to or shared with third parties, if applicable.
 - Limit use and disclosure of Sensitive Personal Information for any purpose other than the pre-approved business purposes identified in the privacy law. Our use of Sensitive Personal Information is already limited to the approved business purposes identified above.

Requests can be submitted by calling our toll-free number (833) 471-0140 or through our [online request form](#). You can also opt out of having Personal Information shared through third party cookies and pixels by clicking on the “[Do Not Share My Personal Information](#)” link. Additionally, when we detect a GPC signal from a user’s browser within California, we stop sharing the user’s personal data online with other companies (except with our service providers). You can learn more about the GPC and how to enable it in your browser from the [Global Privacy Control](#) website.

Only you, or a person that you authorize to act on your behalf, may make a verifiable request related to your Personal Information. Except where you have provided an agent with a Power of Attorney pursuant to Sections 4000 – 4465 of the California Probate Code, when using an authorized agent you must: (1) provide the agent with signed permission clearly describing their authority to make a request on your behalf; (ii) verify your own identity; and (iii) directly confirm that you have provided the authorized agent permission to submit the request. That agent must also be able to verify their identity with us and provide us with their authority to act on your behalf.

The verifiable request initiated by you or your authorized agent must:

- Include your full legal name, email, and phone number, which we will need to contact you in order to verify that you are the person about whom we collected Personal Information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request and confirm the Personal Information relates to you. Making a verifiable request does not require you to create an account with us. One of our

representatives will contact you in order to verify your identity. You may need to provide additional information in order to verify your request. Depending on the nature of the request, we may require additional verification actions be taken, including but not limited to providing a signed declaration under penalty of perjury that you are the person whose Personal Information is the subject of the request. We will only use this information to verify the requestor's identity or authority to make the request.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Engage in employment related activities and take actions reasonably anticipated within the context of our employment relationship with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Exercise a right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *seq.*).
- Enable solely internal uses that are reasonably aligned with expectations based on your contractual or employment relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We endeavor to respond to a verifiable request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded.

The CCPA provides the right to be free from discrimination if you choose to exercise your rights under the statute, and we will not retaliate against you for the exercise of your rights.

Changes to the Policy

We may modify or update this Policy from time to time. We encourage you to revisit this page often to remain fully informed of our Policy or you can contact us at any time to obtain the latest copy of this Policy.

Questions

If you have any questions or concerns about this Policy, please contact Employer's Human Resources Department by e-mailing askHR@embered.com.