



California Applicant and Employee Privacy Notice

Last Updated: September 2026

This California Applicant and Employee Privacy Notice describes how Raceway Car Wash (“Raceway,” “we,” or “us”) collects, uses, and discloses personal information about job applicants, employees, and other members of our workforce who reside in the State of California (“you”). We provide this Notice to comply with the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the “CCPA”), and other California privacy laws. Terms defined in the CCPA have the same meaning when used in this Notice.

Information We Collect

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual (“personal information”). We collect and use this information for human resources, employment, benefits, health and safety, business, and legal-compliance purposes. The categories of personal information we collect, and the business purposes for which we use them, are described below.

Personal Information Category	Business Purpose
Identifiers — such as your name, contact information, date of birth, gender, signature, Social Security number, and driver’s license or state identification number, and similar information for your dependents and beneficiaries.	• Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks • Maintain and administer payroll and employee benefit plans, including enrollment and claims handling • Maintain personnel records and complying with record retention requirements • Communicate with employees and their emergency contacts and plan beneficiaries • Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws • Ensure employee productivity and adherence to Company policies • Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy • Respond to law enforcement or legal requests and as required by applicable law or court order • Exercise or defend the legal rights of the Company and its employees, customers, contractors, and agents
California customer-records information — (Cal. Civ. Code § 1798.80), such as name, signature, Social Security	• Same purposes as for Identifiers

Personal Information Category	Business Purpose
number, physical description, photograph, address, telephone number, driver's license or state ID number, insurance policy number, education, employment and employment history, membership in professional organizations, licenses and certifications, bank account number, credit card number, debit card number, or any other financial, medical or health insurance information.	
Protected classification characteristics — under California or federal law, such as age (40 or older), race, color, ancestry, national origin, citizenship, religion, marital status, medical condition, physical or mental disability, sex (including gender, gender identity or expression, and pregnancy), sexual orientation, reproductive health decision-making, military or veteran status, or genetic information.	• Comply with federal and state equal employment opportunity laws • Perform workforce analytics, data analytics, and benchmarking • Conduct internal audits, grievances, and suspected violations of Company policy • Exercise or defend the legal rights of the Company and its employees, customers, contractors, and agents
Internet or other similar network activity information, including all activity on the Company's information systems (such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and	• Facilitate the efficient and secure use of Company information systems • Ensure compliance with Company information systems policies and procedures. • Comply with applicable state and federal laws • Prevent unauthorized access to, use, or disclosure or removal of the Company's property, records, data, and information • Enhance employee productivity

Personal Information Category	Business Purpose
passwords) and all activity on communications systems (such as phone calls, call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of company-issued devices).	• Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy • Exercise or defend the legal rights of the Company and its employees, customers, contractors, and agents
Geolocation data — such as GPS location data from company vehicles and equipment.	• Improve safety of employees, customers, and the public regarding use of the Company property and equipment • Prevent unauthorized access, use, or loss of the Company property • Improve efficiency, logistics, and supply chain management • Ensure employee productivity and adherence to the Company's policies • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company's policy
Sensory and surveillance data — audio, electronic, visual, or similar information, including call monitoring, video surveillance, and audio and video recordings of employees and other workforce members at or near cashier stations, transaction areas, customer-facing areas, and other Company premises where recording equipment is installed. These recordings may capture your image, voice, conversations, interactions with customers or other personnel, cash-handling activity, payment-	• Prevent unauthorized access, use, or loss of the Company property • Promote workplace employee, customer, and premises safety and security • Improve customer service • Document, verify, and monitor customer transactions conducted at cashier stations • Monitor compliance with cash-handling, payment-processing, customer-service, loss-prevention, workplace-safety, and other Company policies • Investigate transaction discrepancies, customer complaints, employee concerns, suspected misconduct, theft, fraud, safety incidents, policy violations, and legal claims • Train employees, evaluate service interactions, and improve business operations • Exercise or defend the legal rights of the Company and its employees, customers, contractors, and agents

Personal Information Category	Business Purpose
transaction activity, and other activity occurring in recorded areas..	
Professional or employment-related information — such as employment application information (work history, academic and professional qualifications, educational records, references, and interview notes, background check, drug testing results, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information, leave of absence information including religious, military and family obligations, health data concerning employee and their family members.	• Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding • Design and administer employee benefit plans and programs, including for leaves of absence. • Maintain personnel records and comply with record retention requirements. • Communicate with employees and their emergency contacts and plan beneficiaries. • Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Prevent unauthorized access to or use of the Company's property, including its information systems, electronic devices, network, and data. • Ensure employee productivity and adherence to the Company policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy. • Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development • Exercise or defend the legal rights of the Company and its employees, customers, contractors, and agents
Non-public education information — such as education records, degrees, and vocational certifications.	• Evaluate suitability for hire, promotion, or transfer
Inferences — drawn from the information above to create a profile or summary reflecting, for example, your preferences, aptitudes, and characteristics.	• Engage in human capital analytics, including to identify correlations about individuals and job success, analyze data to improve retention and productivity, and analyze employee preferences to inform human resources policies and procedures • Conduct applicant reference checks to assist in hiring decisions
	•



We retain the above information for the duration of your application or employment relationship and afterward for the period necessary to fulfill the purposes described in this Notice and to comply with our legal, tax, accounting, and recordkeeping obligations.

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
 - Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
 - Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

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

- Directly from you. For example, from documents beginning from the job application process, on-boarding documents, and documents necessary for eligibility and participation in employment benefits.
- Indirectly from our service providers or their agents. For example, through information we collect from our service providers in the course of receiving services to them – such as employment agencies, on-line job resources (including Indeed.com), or background check companies.
- Directly and indirectly from activity on our website (www.racewaycarwash.com). For example, from submissions through our website portal or website usage details are collected automatically.
- Directly and indirectly from Company facilities, systems, equipment, and devices. For example, from security cameras, audio and video recording equipment, point-of-sale systems, cashier-station systems, access-control systems, and other workplace systems used in connection with Company operations, customer transactions, safety, security, loss prevention, and policy compliance.

If you applied for a position with the Company through a third-party job platform such as Indeed.com, that platform may collect personal information from you and share it with us to process your application. We encourage you to review the platform's own privacy policy to understand its data practices, which were disclosed to you before submitting your application and which are separate from the Company's policy.

How We Use Personal Information

In addition to the specific business purposes listed above, we may use, disclose, or retain the personal information we collect to:

- Comply with applicable laws and regulations
- Recruit and evaluate job applicants
- Manage your employment relationship with us, including for:
 - onboarding processes;
 - timekeeping, payroll, and expense report administration;
 - employee benefits administration;
 - employee training and development requirements;



- the creation, maintenance, and security of your online employee accounts;
- reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill;
- workers' compensation claims management;
- employee job performance, including goals and performance reviews, promotions, discipline, and termination;
- other human resources purposes; and
- Manage and monitor access to company facilities, equipment, and systems
- Conduct internal audits and workplace investigations, and enforce company policies
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company.
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Perform workforce analytics and benchmarking
- Administer and maintain the Company's operations, including for safety purposes.
- Exercise or defend the legal rights of the Company and its employees, and affiliates, customers, contractors, and agents.
- Record, monitor, review, and use audio and video recordings from cashier stations and related areas for transaction verification, customer service, employee and customer safety, security, loss prevention, employee training, operational improvement, policy enforcement, investigations, legal compliance, and the exercise or defense of legal rights.

We will not collect additional categories of personal information, or use the personal information we collected for materially different or incompatible purposes, without first providing you notice.

How We Disclose Personal Information

We may disclose your personal information for a business purpose. When we do, we enter into a contract that limits the recipient's use of the information to the services being provided. We may disclose your personal information to:

- Service providers — such as payroll, benefits, background-check, information-technology, security, surveillance, loss-prevention, point of sale, payment processing, and claims-management providers
- Third parties you or your authorized agent direct us to share it with
- Government agencies, law enforcement, or others as required by law or to establish or defend legal rights

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes that purpose.

We may disclose the following categories of personal information for a business purpose:

- California Customer Records personal information categories.
- Protected classification characteristics under California or federal law.
- Professional or employment-related information.
- Sensory and surveillance data, including audio and video recordings from cashier stations and other recorded areas.



We disclose your personal information for a business purpose to the following categories of third parties:

- Service providers.
- Third parties to whom you or your agents authorize us to disclose your personal information.

We will not knowingly sell (as defined by CCPA) the personal information, including any sensitive personal information, we collect about our employees or applicants for employment or share it with third parties for cross-context behavioral advertising.

Audio and Video Recording

Raceway currently uses, and may continue to use, audio and video recording at or near cashier stations and related transaction areas. These recordings are used in connection with customer transactions and cashier-station operations and may capture employees, applicants, contractors, customers, and other individuals who are present in recorded areas.

Recordings may include your image, voice, conversations, interactions with customers or other personnel, cash-handling activity, payment-transaction activity, and other conduct or activity occurring in recorded areas. Raceway uses these recordings for legitimate business purposes, including transaction verification, customer service, safety and security, loss prevention, employee training, operational improvement, policy compliance, workplace investigations, legal compliance, and the exercise or defense of legal rights.

Raceway may review, retain, disclose, or otherwise use these recordings as described in this Notice and in accordance with applicable law and Company policy.

Data Security

We implement reasonable physical, technical, and administrative safeguards to protect your personal information. Access to personal data is restricted to authorized personnel only and is stored securely. Measures include encryption, access controls, and monitoring of network and device activity, including appropriate safeguards for audio and video recordings and related surveillance systems, to prevent unauthorized access.

Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents. If you are a California resident, you have the following rights pursuant to the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

- Right to Know. The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected, shared or sold about you, (2) the categories of sources from which the personal information was collected, (3) the business purpose for which we use this information, and (4) the categories of third parties with whom we disclose or have disclosed your personal information;
- Right to Access. The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of personal information we have collected about you;



- Right to Delete. The right to request, up to 2 times in a 12-month period, that we delete personal information that we have collected from you, subject to certain exceptions;
- Right to Correct. The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;
- The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and
- The right to not be discriminated or retaliated against for exercising any of the above rights.
- Right to Restrict the Use of Sensitive Personal Information. You have the right to restrict the use of your sensitive personal information.
- Right to Access Information on Automated Decision-Making: You have the right to access information collected through automated decision-making. Additionally, you can opt-out of our use of automated decision-making related to your personal information.
- Right to Data Portability: You may request a copy of your personal data in a portable and accessible format.

You can submit any of the above types of requests by any of the options below:

- Emailing Human Resources at humanresources@racewaycarwash.com
- Calling 602-900-1731
- Mailing Raceway Car Wash, Attn: Human Resources, 2850 E. Camelback Rd., Suite 330, Phoenix, AZ 85016

How We Will Verify That it is Really You Submitting the Request:

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us.

Responding to your Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a



good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we cannot comply with a request, if applicable.

If You Have an Authorized Agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney, or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

We will respond to any requests in accordance with applicable law, and there may be circumstances where we are not able to comply with your request.

Consent to Terms and Conditions

By applying for a position with the Company or submitting any information for purposes of being considered for or inquiring about employment with the Company, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to This Notice

This Notice was last updated on the date shown above. We reserve the right to amend this privacy policy and notice at our discretion and at any time. When we make changes to this privacy notice, we will notify you by email, U.S. Mail, providing a hyperlink, or posting.

Contact Us

If you have questions or comments about this Notice or our privacy practices, or if you need to access this Notice in an alternative format due to a disability, please contact Human Resources by email at humanresources@racewaycarwash.com, by phone at 602-900-1731, or by mail at Raceway Car Wash, Attn: Human Resources, 2850 E. Camelback Rd., Suite 330, Phoenix, AZ 85016.