

Privacy Notice: Employees and Job Applicants

This notice describes (i) the categories of personal information that may be collected by Boise Cascade ("Company," "we," or "us") in connection with your employment or application for employment, (ii) the purposes for which such personal information may be collected, used, and disclosed by us, (iii) with whom we may share your personal information, and (iv) the length of time we may retain your personal information.

CATEGORIES OF PERSONAL INFORMATION COLLECTED

As a Company employee or job applicant, we may collect the following categories of personal information about you:

- Identifiers and Contact information. This category includes names, addresses, telephone numbers, mobile numbers, email addresses, dates of birth, Social Security numbers, driver's license or state identification numbers, bank account information, access/identification badges, profile pictures, and other similar contact information and identifiers.
- Protected classification information. This category includes characteristics of protected classifications under California or federal law, such as your age, race, national origin, citizenship, and marital status.
- Internet or other electronic network activity information. This category includes without limitation:
 - 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 passwords, and
 - all activity on communications systems including phone calls, call logs, voice mails, 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.
- Geolocation data. This category includes GPS location data from Company-issued mobile devices and company-owned vehicles.
- Audio, electronic, visual, thermal, olfactory, or similar information. This category includes, for example, information collected from cameras, thermometers, and similar devices, which may be used for call monitoring or video surveillance in our facilities.
- Biometric information. This category includes "biometric identifiers" (such as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and "biometric information" (any information based on an individual's biometric identifier used to identify an individual), as those terms are defined under applicable law, including the Illinois Biometric Information Privacy Act (BIPA), the Texas Capture or Use of Biometric Identifier Act (CUBI), and the Washington biometric privacy law. This includes information collected using biometric equipment, devices, or software that may record your time worked, when you enter or exit facilities or rooms, when you access or use equipment, or purposes disclosed to you at the time of collection. Additional consent, notice, and retention requirements applicable to biometric information are described below under "Biometric Information: Consent, Use, and Retention."

- Professional and employment-related information. This category includes without limitation:
 - data submitted with employment applications including salary history, employment history, employment recommendations, etc.,
 - background check and criminal history,
 - work authorization information,
 - fitness for duty data and reports,
 - performance and disciplinary records,
 - salary and bonus data,
 - benefit plan enrollment, participation, and claims information, and
 - leave of absence information including religious and family obligations, physical and mental health data concerning employee and his or her family members.
- Education information. This category includes education history, resume or CV information, and any employment related certifications, licensures, or related qualifications.
- Limited medical information. This category includes without limitation:
 - symptoms, test results, and other indicators of exposure to the coronavirus (COVID-19) and related vaccination status information,
 - fitness for duty data and reports,
 - leave of absence information including family obligations, physical and mental health data concerning employee and his or her family members, and
 - travel information and information regarding close contacts.

Please note that medical information collected from you in connection with Company benefits and the voluntary Company wellness program are discussed in the “Notice of HIPAA Privacy Practices for Personal Health Information” and “Notice Regarding Wellness Program,” respectively. Medical information collected in connection with the wellness program is maintained separately from your personnel records.
- Inferences drawn from the personal information in the categories above.

SOURCES OF PERSONAL INFORMATION

The Company collects personal information from the following categories of sources:

- Directly from you, including information you provide in applications, forms, surveys, and communications;
- From third-party service providers, including background check vendors, and staffing agencies;
- From government agencies;
- From publicly available sources; and
- From Company information systems and devices.

SENSITIVE PERSONAL INFORMATION COLLECTED

Some of this personal information collected about you is considered Sensitive Personal Information, including your:

- social security, driver's license, state identification card, or passport number,
- financial account information that allows access to an account, including log-in credentials, financial account numbers, passwords, etc.,
- precise geolocation,
- racial or ethnic origin, citizenship, or immigration status, religious or philosophical beliefs, or union membership,
- content of mail, email, and text messages unless the Company is the intended recipient of the communication,
- genetic data,
- uniquely identifying biometric information, and
- information concerning health and sex life or sexual orientation.

YOUR RIGHTS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

If you are a California employee or job applicant, you have the following rights under the CCPA (as amended by the California Privacy Rights Act), subject to applicable legal exceptions and verification requirements:

- Right to Know. You have the right to request that the Company disclose the categories of personal information collected about you, the categories of sources from which it was collected, the business or commercial purposes for collecting, selling, or sharing it, the categories of third parties to whom it was disclosed, and the specific pieces of personal information collected about you.
- Right to Delete. You have the right to request deletion of personal information collected from you, subject to exceptions permitted by law.
- Right to Correct. You have the right to request correction of inaccurate personal information maintained about you.
- Right to Limit Use of Sensitive Personal Information. You have the right to direct the Company to limit its use and disclosure of your Sensitive Personal Information to the purposes permitted by Cal. Civ. Code § 1798.121.
- Right to Non-Discrimination. The Company will not discriminate against you for exercising your CCPA/CPRA privacy rights.
- Right to Opt Out of Sale or Sharing. You have the right to opt out of the sale or sharing of your personal information. The Company currently does not sell your personal information for monetary or other valuable consideration or share it for cross-context behavioral advertising, but this right applies if the Company's practices change.
- To submit a request to exercise these rights, you may call 1-844-823-2382 or use email privacyofficer@bc.com.

PURPOSES FOR WHICH PERSONAL INFORMATION IS USED

The purposes for which we use your personal information are limited to:

- Collecting and processing employment applications, including confirming eligibility for employment, background and related checks, onboarding, and related recruiting efforts.

- Processing payroll, other forms of compensation, and employee benefit plan and program design and administration including enrollment and claims handling and leave of absence administration.
- Maintaining physician records and occupational health programs.
- Maintaining personnel records and record retention requirements.
- Communicating with employees and/or employees' emergency contacts and plan beneficiaries.
- Complying with applicable state and federal health, labor, employment, benefits, workers compensation, disability, equal employment opportunity, workplace safety, and related laws, guidance, or recommendations.
- Preventing unauthorized access to, use, or disclosure/removal of the Company's property, including the Company's information systems, electronic devices, network, and data.
- Ensuring and enhancing employee productivity and adherence to the Company's policies.
- Providing training and development opportunities.
- Investigating complaints, grievances, and suspected violations of Company policy.
- Designing, implementing, and promoting the Company's associate engagement programs.
- Facilitating the efficient and secure use of the Company's information systems.
- Ensuring compliance with Company information systems policies and procedures.
- Improving safety of employees, customers, and the public with regard to use of Company property and equipment.
- Improving efficiency, logistics, and supply chain management.
- Improving accuracy of time management systems, attendance, including vacations, sick leave, and other absence monitoring.
- Evaluating an individual's appropriateness for a participation position at the Company, or promotion to a new position.
- Responding to and managing any legal claims against the Company and/or its personnel, including civil discovery in litigation.
- Facilitating other business administrative functions and strategic activities, such as risk management, information technology and communications, financial management and reporting, human resources activities, workforce, and succession planning, mergers, and acquisition activities; and maintenance of licenses, permits and authorization applicable to Company operations.
- Conducting identity verification, authentication, security, fraud prevention, workplace safety, access control, or other legitimate business purposes.

Please note that the Company may add categories of personal information it collects and the purposes it uses personal information. In that case, the Company will inform you. We reserve the right to amend this Notice at any time.

BIOMETRIC INFORMATION: CONSENT, USE, AND RETENTION

The Company may collect certain biometric identifiers including facial geometry scans, fingerprints, and voice prints for the following specific purposes: identity verification, authentication, security, fraud prevention, workplace safety, workplace communications, access control, or other specific purposes, which shall be disclosed at the time of collection. The

Company may also use biometric identifiers to record your time worked, when you enter or exit facilities or rooms, or when you access or use equipment at company facilities.

Biometric identifiers and biometric information will be retained for (a) the duration of your employment term or thereafter as reasonably required by legal and regulatory requirements and Company retention schedules; or (b) until the initial purposes for collecting such data has been satisfied, whichever occurs first.

The Company will not sell, lease, trade, or otherwise profit from your biometric identifiers or biometric information.

The Company will not disclose or redisclose your biometric identifiers or biometric information to any third party without first obtaining your written consent unless such disclosure is required by law or pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

The Company maintains a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such data has been satisfied or within three (3) years of your last interaction with the Company, whichever occurs first. A copy of this policy is available at [Privacy Policy - Boise Cascade \(www.bc.com/privacypolicy\)](http://www.bc.com/privacypolicy).

- For Illinois residents, in no event will biometric data be retained longer than three (3) years after your last interaction with the Company, unless otherwise legally required.
- For employees and applicants located in Texas, the Company will not disclose biometric identifiers to a third party unless: (i) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (ii) the disclosure completes a financial transaction requested or authorized by the individual; (iii) the disclosure is required or permitted by a federal statute or by a state statute; or (iv) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.
- For employees and applicants located in Texas, the Company will destroy biometric identifiers within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires. If the biometric identifier was collected for a security purpose, the purpose is presumed to expire on termination of the employment relationship.

The Company will store, transmit, and protect biometric identifiers using reasonable care and in a manner that is the same as or more protective than the manner in which the Company stores, transmits, and protects other confidential information in the Company's possession.

SALE OR SHARING OF PERSONAL INFORMATION

To carry out the purposes outlined above, the Company may share personal information, including sensitive personal information, with service providers such as background check vendors, third-party staffing vendors and information technology vendors, outside legal counsel, and state or federal governmental agencies.

To ensure consistency and objectivity, personal information released to Company personnel, other than those described above, or to parties outside the Company is strictly limited to:

- i. Name
- ii. Work location
- iii. Position held

- iv. Length of employment
- v. Current status, including termination date or retirement date, if applicable.

The release of any additional information requires written authorization from the associate, with the following exceptions:

- i. In response to reference check requests from other employers, in addition to the information that can be provided without a release (listed in the preceding paragraph), the rate of pay may be confirmed but should not be volunteered. To be consistent with the Federal Motor Carrier Safety Regulations requiring reference checks on commercial drivers and to meet good Company citizenship objectives, job-related driving information may also be released
- ii. Releases based on business necessity to outside agents retained by the Company, which include but are not limited to third parties, such as auditors, insurance carriers, actuaries, and attorneys
- iii. Reporting to governmental agencies as required by law and based upon standards established by the Legal Department
- iv. Disclosures in certain circumstances to bargaining representatives (unions) as required under the National Labor Relations Act. Employers are required, as part of their obligation to bargain in good faith, to furnish unions with all information that is probably or potentially relevant to the performance of their function as exclusive bargaining agents for represented associates. Because access to some of this information might normally be strictly limited under the provisions of this policy, any questions regarding what the Company is legally required to release should be directed to the Legal Department. Affected associates will be notified prior to release of the information
- v. Releases of any and all information, except individual medical claims information, to the purchaser of a plant, division, subsidiary, joint venture, or any entity of the Company where the purchaser continues the employment of former associates. Medical claims data in its possession which is needed to continue future claims processing for former associates and their dependents will be provided to the purchaser or their claims representative on an entire group basis. Such data includes amounts accumulated toward plan deductibles and plan limits. Individual medical claims information regarding former associates and their dependents will be provided to the purchaser, or their claims representative, only upon written release from the patient (or associate if the patient is a minor dependent)
- vi. Releases in response to subpoena or other court order under the direction of the Legal Department

The Company does not sell your personal information for monetary or other valuable consideration, and does not share your personal information for cross-context behavioral advertising. If the Company's practices change such that the Company begins to sell or share personal information as so defined, the Company will update this notice and provide associates with the ability to opt out before any such sale or sharing occurs.

DATA RETENTION

The retention period for each category of personal information depends on the category of personal information and the purpose for which it was collected. Each category will be retained for the period stated in the Company's records retention schedule available at [Privacy Policy - Boise Cascade \(www.bc.com/privacypolicy\)](http://www.bc.com/privacypolicy). Specific categories may be retained for 10 years following termination of employment as required by applicable law.

FOR MORE INFORMATION

For more information about our privacy practices in regard to employee personal information, please see the Company's Privacy Policy at [Privacy Policy - Boise Cascade](#) (www.bc.com/privacypolicy). If you would like to request a copy of the Policy, or if you have questions about this notice or the Company's compliance with applicable privacy laws, please contact the Company's Privacy Officer at privacyofficer@bc.com .