U.S. ASSOCIATE PRIVACY POLICY

This Policy was last updated on December 5, 2022.

Bath & Body Works, Inc., including its subsidiaries and affiliated entities, (the “Company,” "we," "us," or "our") respects your concerns about privacy. This internal U.S. Associate Privacy Policy ("Policy") explains what personal information we collect when you become an associate of the Company, how we use that information, to whom we disclose it, and how we safeguard it.

WHAT DOES THIS POLICY COVER?

This Policy applies to our employees who reside and work in the United States.

We may obtain the following categories of personal information about you (collectively, “employee personal information”):

- Identifiers such as name, work and personal postal address, phone number, email address, emergency contact information, driver’s license or state identification card number, passport number, visa ID number, Social Security number, Social Insurance number, Tax ID number, Employee ID, and signature;

- Other personal information such as demographic and family information, including age, date of birth, gender, veteran status, and dependent information;

- Characteristics of protection classification such as race, ethnicity, marital and family status, disability status, and medical condition;

- Commercial information such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

- Biometrics information;

- Internet or other electronic network activities such as your use of Company IT and communications resources, including timestamp information, IP address, activity logs, and call detail records;

- Geolocation data;

- Photographs, and video and audio recordings;

- Information related to employment, including occupation details, CV information, language and other job-related skills, historical compensation details, previous employment details, and references;

- Education information such as education history, majors, and degrees;

- Inferences drawn from any of the information identified such as preferences, predispositions, behaviors, attitudes, abilities, and aptitudes;

- Sensitive personal information such as racial or ethnic origin, social security number, driver's license or other state identification number, and citizenship or citizenship status;

- Compensation, benefits, and payroll information, including bank account details and salary-related information, payment card information, tax-related information, and information relating to participation in group insurance policies (such as insurance policy number, medical information and health insurance information);

- Information relating to your position, including job title, job description, office location, hire date, termination date, training details, performance evaluation, disciplinary actions, information regarding fitness for work, paid time off or leave of absence, alcohol or drug testing-related information (where permitted by applicable law), and information regarding immigration status and eligibility for work; and

- The content of communications that traverses Company IT and telecommunications resources.

WHEN IS EMPLOYEE PERSONAL INFORMATION COLLECTED, AND HOW IS IT USED?

If you're hired for a position with the Company, we will collect employee personal information during and after the course of your employment with us and use it to administer the employment and post-employment phases of the relationship.

We may incorporate information from your job application into your personnel file, and we may collect employee personal information directly from you. We also collect employee personal information in the course of job-related activities.

We may collect information from third parties (e.g., during the application and recruitment process, in connection with background checks and the onboarding process, and as part of a change in duties or a promotion) to supplement your employee personal information.

We may also collect and use contact information that you provide about people you know (for example, your emergency contacts or people covered by your benefits programs).

We may use your employee personal information for the following purposes:

- Workforce management: managing work activities and personnel generally, including recruiting and employee on-boarding; performing background checks; determining suitability for employment or promotion; determining physical and/or mental fitness for work; reviewing and evaluating performance; determining eligibility for and processing salary increases, bonuses, and other incentive-based compensation; providing employee discounts; providing references; managing attendance, absences, leaves of absences, and vacations; administering payroll and compensation services; reimbursing expenses; administering health, dental, and other benefits; training and development; making travel arrangements; securing immigration statuses; monitoring staff; creating staff directories; investigating suspected misconduct or non-performance of duties; managing disciplinary matters, internal investigations, grievances, and terminations; reviewing staffing decisions; and providing access to facilities;

- Facilities and emergencies: ensuring business continuity; protecting the health and safety of our staff and others; responding to incidents; safeguarding, monitoring, and maintaining our IT infrastructure, telecommunications network, office equipment, facilities, and other property; detecting or preventing theft or fraud, or attempted theft or fraud; and facilitating communication with you and your designated contacts in an emergency;

- Business operations: operating and managing our IT, communications systems and facilities, and monitoring the use of these resources; providing technical support; performing data analytics; improving our services; allocating and managing company assets and human resources; strategic planning; producing promotional videos; managing projects; planning events; compiling audit trails and other reporting tools; maintaining records relating to business activities, budgeting, and managing finances; managing mergers, acquisitions, liquidations, sales, reorganizations or disposals, and integrating with purchasers; and

- Legal and compliance: complying with legal requirements, such as tax, record-keeping and reporting obligations; conducting audits, management and resolution of health and safety matters; complying with requests from government or other public authorities; responding to legal process such as subpoenas and court orders; pursuing legal rights and remedies; defending litigation and managing internal complaints or claims; conducting investigations; and complying with internal policies and procedures.

We may also use monitoring, communications interception, and recording technology to collect information about you and others to protect people and property. For example, we may use video and surveillance technology in our stores and in our facilities; and we may intercept, access, use, and disclose communications (like emails) that traverses our company network and assets (e.g., computers and phones).

ELECTRONIC MONITORING

During the course of employment with the Company, any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee through any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio, camera, or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring or interception at any and all times and by any lawful means.

WHAT INFORMATION DO WE SHARE WITH OTHER ENTITIES (OR WHAT INFORMATION MAY THEY ACCESS BECAUSE OF THE SERVICES THEY PROVIDE)?

We may share your employee personal information (as listed above in "What Does this Policy Cover?") with our subsidiaries and affiliates. We may also share your employee personal information (as listed above in "What Does this Policy Cover?") with service providers or contactors who provide us with services that we find necessary to run our business, and which may directly or incidentally involve your employee personal information. These providers help us do all the things listed above (see When is Employee Personal Information Collected, and How is It Used?), as summarized below:

- Provide workforce management.
- Maintain facilities and respond to incidents and emergencies.

- Maintain business operations.
- Deliver legal and compliance services.

We also may disclose personal information about you (a) if we are required to do so by law or legal process (such as a court order or subpoena); (b) in response to requests by government agencies, such as law enforcement authorities; (c) to establish, exercise, or defend our legal rights; (d) when we believe disclosure is necessary or appropriate to prevent harm or financial loss; (e) in connection with an investigation of suspected or actual illegal activity; or (f) otherwise with your consent.

We reserve the right to share and/or transfer your information in the event we sell or transfer all or a portion of our business assets (including, without limitation, in the event of a merger, demerger, spin off, acquisition, joint venture, reorganization, dissolution, or liquidation).

HOW DO WE PROTECT EMPLOYEE PERSONAL INFORMATION?

We maintain administrative, technical, organizational, and physical safeguards designed to protect employee personal information from accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure, or use.

SUPPLEMENTAL POLICIES FOR CALIFORNIA RESIDENTS

Your Data Rights. If you are a resident of California, you have the right to request, twice in a 12-month period, that we disclose to you the employee personal information we have collected, used, disclosed, and shared about you. In addition, you have a right to request that we delete or correct certain employee personal information.

To submit a request, visit Your Data Rights or call us at 1-866-473-4728. For assistance, contact us via Telecommunications Relay (TRS) Service (TRS) by dialing 711, or by using an Internet Protocol Relay Service. To help protect your privacy and maintain security, we take steps to verify your identity with a high degree of certainty before granting access to specific pieces of personal information or complying with a deletion or correction request. To complete the request, you will need to provide certain verifying information including your associate identification number.

Your authorized agent can also submit a request on your behalf by visiting Your Data Rights. To complete the request, the agent will need certain information about you such as your business email address, date of birth, associate identification number, and other information about you. We will require your authorized agent to identify that it is acting as an agent on your behalf, verify its own identity, and submit proof that the associate has given signed permission for the agent to submit the request.

To the extent permitted by the applicable law, we may charge a reasonable fee to comply with your request.

Right to Non-Discrimination or Retaliatory Treatment for Exercise of Privacy Rights: You, whether as a consumer, employee, former employee, applicant, or contractor, have the right to exercise your privacy rights without receiving discriminatory or retaliatory treatment. If you exercise any of your privacy rights, you will not be treated differently from those who do not exercise their privacy rights.

Sensitive Personal Information: We will only process Sensitive Personal Information where it is necessary for the purposes of carrying out our legal obligations, exercising specific rights as permitted by law, or if you have given the Company consent. Sensitive Personal Information is any information that reveals your race, ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data, personal information of a known child, or precise geographic data.

Retention Policy: We seek to ensure that we retain only necessary information and comply with our legal obligations. The need to retain employee personal information varies widely with the type of information and the purpose for which it was collected. We strive to ensure that this information is only retained for the period to fulfill the purpose for which it was collected and is deleted when it is no longer required per our retention policies. For specific information, please request the Global Records Management Policy.

WHAT IF I HAVE QUESTIONS OR CONCERNS?

If you have questions or concerns about your employee personal information or this Privacy Policy, please contact**:**

Privacy Team
Bath & Body Works, Inc.
3 Limited Parkway
Columbus, OH 43230
privacyoffice@bbw.com

UPDATES TO THIS POLICY

This Policy may be updated periodically to reflect changes in our personal information practices.