



California Worker Privacy Statement January 1, 2023

Graham Holdings Company and its affiliates (“the Company”) respect the privacy of your personal information and take our related compliance and regulatory obligations seriously. This California Privacy Statement (“Statement”) describes the categories and uses of the Personal Information (as defined below) of Company employees, independent contractors and job applicants who reside in California (collectively “California Workers”) as required by the California Consumer Privacy Act (“CCPA”) as amended by the California Privacy Rights Act (“CPRA”). The term “California Workers” includes current and former job applicants, independent contractors, temporary staff, interns, company officers, directors, emergency contacts, and benefits recipients in addition to employees solely for the purpose of this Statement.

The Company receives Personal Information, including Sensitive Personal Information, from and about you during the course of interviewing, hiring and employing or engaging you. We also may collect Personal Information about your related family members, dependents and beneficiaries in connection with benefits processing or obtaining emergency contacts. “Personal Information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

The Company collects, uses, and discloses this sensitive personal information only as necessary to perform the services reasonably expected by an employee, and for business purposes permissible for sensitive personal information under the CCPA and CPRA.

The Company does not sell or share California Workers’ Personal Information, including Sensitive Personal Information, including that of individuals under age 16.

Categories of Personal Information Collected

(Some information may overlap categories)

Category	Examples
Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, or other financial information, medical information, or health insurance information.
Protected classification characteristics under California or federal law.	Age (40 years or older), race, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status.



California Worker Privacy Statement
January 1, 2023

Internet or other similar network activity.	Email sent or received on the Company network or on your Company computer, browsing history, search history, and information on your interaction with a website, application, or advertisement while operating on the Company network.
Geolocation data	Internet protocol address, which may indicate general location.
Sensory data.	Photos, videos, voicemail, and meeting recordings
Professional or employment-related information.	Job title, business site, supervisor, work schedule and status, compensation information, benefit information, training and development information, employment duration, current or past job history or performance evaluations, certification information, special competencies or work accomplishments and other relevant information.
Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, predispositions, behavior, attitudes, and aptitudes.
Sensitive Information	Social Security Number, driver's license number, state identification card number, or passport number; racial or ethnic origin; religious or philosophical beliefs; personal information collected and analyzed concerning the California Worker's health; sex life or sexual orientation.

Purposes for Processing Your Personal Information

The processing of your Personal Information enables the Company to perform its role as an employer and/or for the purposes of engaging you, including fulfilling its legal obligations under applicable laws and as necessary in connection with the Company's performance of its employment and/or other worker obligations. Without this information, it would not be possible for the Company to manage the workforce and meet applicable legal obligations. The Company processes certain Personal Information for its business interests, including, but not limited to, the following:

1. applicant recruiting and employee on-boarding;
2. payroll administration and independent contractor payment processing;
3. pension administration;
4. health administration/health insurance benefits;
5. life insurance benefits;
6. expense reimbursement and management;
7. contacting others in the event of an emergency;



California Worker Privacy Statement

January 1, 2023

8. making information available on the intranet and to facilitate communication between and among the Company workforce;
9. administration and management of your access to information technology systems;
10. time entry and leave management;
11. training, appraisal, and development, such as personality and aptitude tests (e.g., DiSC and Strengths Finder), performance records and disciplinary records;
12. employee and staff surveys;
13. equal opportunities monitoring;
14. any Company benefit administration, including equity-related plans and benefits;
15. for public relations purposes and in connection with the performance of your duties (e.g., the Company may send your contact information to customers and potential customers as part of the sales process so they can contact you); and
16. to comply with applicable laws and legal obligations, including without limitation:
 - a. to maintain the ethics hotline;
 - b. to respond to governmental inquiries or requests from public authorities;
 - c. to comply with valid legal process or discovery obligations;
 - d. to protect the rights, privacy, safety or property of the Company, its workers or the public if such a disclosure is proportionate in the individual case;
 - e. to permit the Company to pursue available remedies or limit the damages that the Company may sustain;
 - f. to respond to an emergency; and/or
 - g. to comply with applicable regulations, policies and procedures.

In some cases, The Company uses the services of suppliers (e.g., benefits providers). As a result, your personal information will be provided to suppliers engaged by The Company that need access to it to provide the services for which they have been engaged.

We disclose the personal information to the following categories of persons:

- Service providers and contractors that process personal information on our behalf pursuant to a written contract.
- To law enforcement and other third parties to address legal obligations.
- To third parties at your direction to fulfill requests by you or with your consent.



California Worker Privacy Statement

January 1, 2023

- To third parties in connection with, or during negotiations of, any proposed or actual merger, purchase, sale or any other type of acquisition.

We retain each category of personal information, including sensitive personal information, in accordance with our Graham Holdings Company Records Retention Policy for the length of time that is reasonably necessary for the purpose for which it was collected, and as necessary to administer benefit plans, comply with our legal obligations, resolve disputes, prevent fraud, and enforce our agreements.

Your Rights

The CPRA provides California residents with specific rights regarding their personal information. This section describes those rights. We do not discriminate against California Workers who exercise any of their rights described in this Privacy Notice.

Request to Access Your Personal Information (Right to Know)

You have the right to request that we disclose certain information to you about our collection, use, and disclosure of your personal information over the past 12 months.

As part of our verification process of your request we ensure reasonable measures are in place to detect fraudulent requests and prevent unauthorized access to your personal information. We are required to verify your identity, and the identity of your authorized agent, if the request is submitted via an agent by associating the information provided in the request to any personal information previously collected by us or use a third-party identity verification service.

Once we confirm your verifiable request, we will disclose to you, consistent with your request:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- Specific pieces of personal information we collected about you, if requested.

Requests to Delete Your Personal Information (Right to Request Deletion)

You have the right to request that we delete any of your personal information that we have collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable request, we will delete (and direct our service providers to delete) your personal information from our records, unless doing so violates federal or state law, or prevents us from providing obligatory services to you.

If we deny your deletion request, we will notify you in writing of the reason.

Requests to Correct Your Personal Information (Right to Request Correction)

You have the right to request that we correct any of your personal information that we have collected from you. If you have an active account, you may be asked to “self-serve” the request. Otherwise, once we receive



California Worker Privacy Statement

January 1, 2023

and confirm your verifiable request, we will correct (and direct our service providers to correct) your personal information in our records.

Submitting a Request

To exercise the rights described above, you can contact us by submitting your request to your HR department or through the California Privacy Policy contact methods for your business.

Only you or your authorized agent may make a verifiable request related to your personal information. If you use an authorized agent to submit a request on your behalf, we may require that you (1) provide the authorized agent written permission to do so, and (2) provide a copy of the authorization or provide a copy of a power of attorney that complies with California Probate Code sections 4000 to 4465 so that we can verify the identity of the authorized agent.

In verifying requests, we employ reasonable measures to detect fraudulent requests and prevent unauthorized access to your personal information. To meet our obligations, we are required to verify your identity, and the identity of your authorized agent, if the request is submitted via an agent, by associating the information provided in your request to personal information previously collected by us.

If we suspect fraudulent or malicious activity on or from the password-protected account, we may decline a request or request that you provide further verifying information.

You may only make a verifiable request twice within a 12-month period. The verifiable request must:

- Provide sufficient information that allows us to verify you are the person about whom we collected personal information and, if applicable, provide necessary documentation about your authorized agent.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

Responding to Requests

Upon receiving your request to know or a request to delete, we will process your request or notify you if the request requires an extension or will be denied. If we only comply with your response in part, we will explain the reasons why. We attempt to process requests within 45 days after receipt. If we require additional time beyond 45 days, we will inform you of the reason and the extension period.

If you have any questions about this Privacy Policy or our information-handling practices, please contact us by email as follows: privacy@ghco.com.