.

Privacy Policy for California Residents

Purpose of this privacy notice

AAR Corp. and its affiliated entities ("**AAR**", "**we**", "**our**" or "**us**") is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect, use, and share personal information about Californian employees before, during, and after your working relationship with us. It applies to all permanent and temporary employees, workers, contractors and any other individuals who are working for AAR but are not directly employed ("**staff member"** or "**you**") who live in California. To be clear, this privacy notice does not apply to any staff member who does not live in California.

Please read this privacy notice carefully. If you have any questions, please contact our Human Resources representative, or a member of the Law Department.

1. Information we collect about you

For the purposes of this privacy notice, "**personal information**" means any information about an identified or identifiable natural person regardless of whether it is held in paper, electronic or any other format.

We collect, maintain, and use different types of personal information in the context of our relationship or potential relationship with you. We also collect certain "special categories" of more sensitive personal information where permitted by applicable law.

The following provides examples of the type of information that we collect from you and how we use the information.

Context	Categories of Information	Primary Purpose for Collection and Use of Information
Benefits	Wage and benefit information, including but not limited to salary, bonus, additional pay, variable compensation, annual leave, pension and related compensation history and benefits information.	To provide employee benefits, including compensation, health insurance, expense reimbursements, etc.
CCTV	CCTV footage and other information obtained through electronic means such as swipe card records.	To protect AAR's property, and maintain the security of information held by AAR.
Certifications and Qualifications	We collect information from individuals who have access to our facilities and equipment including licensing and certification, and when applicable, nationality and citizenship.	To secure our facilities and equipment, and track those individuals with who have access for security and maintenance purposes. We may also be required by law to validate and record information about the individuals that access our facilities and equipment.
Contact Details	Personal contact details such as name, title, addresses, telephone numbers, and work and personal email address.	To communicate with you. In certain circumstances, we are also required to collect this information to comply with law.
Electronic Communications	Information about your use of our information and communications systems.	To monitor your use of our information and communication systems, provide for the security of the IT system, and to ensure compliance with our IT policies.
Government	Social security numbers, tax payer	To comply with law.

Identification	identification numbers, passport, or other government identifiers.	
Health Related	Information about your health, including any medical condition, health and sickness records, details of any absences from work (other than holidays), including time on statutory parental leave and sick leave.	To ascertain your fitness to work and manage sickness absence. To comply with legal obligations related to health and safety. To provide health benefits such as insurance.
Identification	Name, date of birth, and driver's license. In some states as applicable by law, we collect an algorithmic digital representation of biometric information.	To identify you personally, including for time and attendance management. In some instances, we are also required to collect this information to comply with law.
Investigations	Details of any disciplinary investigations and proceedings, or of investigations following an alert.	To gather evidence for possible grievances or disciplinary hearings, or to make arrangements for the termination of our working relationship if warranted.
Other Special Categories Of Sensitive Information	Information about your gender, race, ethnicity, sexual orientation, religious beliefs, veteran status, health and disability data, and trade organization data.	To comply with government regulations related to promoting and monitoring equal opportunities and diversity (if permissible under local applicable law) and to manage personnel representation elections and meetings.
Payroll, Pension, and Taxes	Payroll information, including but not limited to social security number or equivalent, tax status information (i.e., marital status, dependents, etc.), payroll records, bank account details, direct deposit/credit arrangements, and information about pension plans.	To calculate and pay your salary, tax, social security, and pension contributions. In some jurisdictions, to comply with our legal obligations.
Photographs	Photographs	To maintain external and internal directories and/or a security badge.
Recruitment	Recruitment information, including copies of right to work documentation such as citizenship, work permit or visa; references and other information included in a CV, resume, or cover letter or as part of the application process; criminal background; references and interview notes; letters of offer and acceptance of employment, and employment agreements.	To make a decision about your recruitment or employment.
Terms of Employment	Employment records including job titles/duties, job location, working arrangements, seniority data, employee identification number, performance ratings, hire/re-hire date, termination date, job history, training records, professional memberships, and business travel arrangements.	To manage our business, including accounting and auditing; to conduct performance reviews, manage performance and determine performance requirements; to make decisions about salary reviews and compensation; to assess qualifications for a particular job or task, including decisions about promotions; to make decisions about your continued employment or engagement. To provide salary and benefits to certain employees.
Training	We collect information from individuals concerning the training and qualifications that they receive from us, or from third parties.	To understand and record the qualifications and training of the individuals that work with us. We may also be required by law, or by contract, to share the training or qualification of certain staff with third parties such as regulators or clients. We may also choose to share the training or qualification of certain staff with third parties as part of our effort to develop business.

In addition to the information that we collect from you directly, we may also receive information about you from other sources, including third parties, business partners, our affiliates, or publicly available sources. For example, if you submit a job application, or become an employee, we may conduct a background check or collect information from your references or previous employers.

2. How we collect your personal information

We collect personal information about staff members through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider where background checks are permitted. In addition, we may sometimes collect additional information from third parties including former employers, personal and professional references, credit reference agencies or other background check agencies, or government agencies (where permitted).

We will also collect additional personal information in the course of job-related activities throughout the period of you working for us. This may include monitoring communications and use of company IT equipment and systems, or from other staff members or supervisors.

3. Monitoring use of company IT equipment and systems

In the course of conducting our business, we may – under conditions permitted by applicable law- monitor employee activities and our premises and property. For example, some of our locations are equipped with surveillance cameras. Where in use, surveillance cameras are for the protection of employees and third parties, and to protect against theft, vandalism, safety and damage to AAR's property. They do not aim at controlling the working activity of the individual employee. Recorded images are typically destroyed and not shared with third parties unless there is suspicion of a crime or wrongdoing, in which case they may be turned over to the police, or other appropriate government agency or other appropriate third parties.

Additionally, pursuant to our Information Technology Policy (Policy No. 1.07.003), and where permitted by law, AAR has the ability to monitor all business communications, including, without limitation, phone, internet browsing, email, instant messaging, and VoIP. For the purposes of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you if you include such information in a business communication. By carrying out such activities using AAR's facilities you acknowledge that sensitive personal data about you may be revealed to AAR by such monitoring. For more information about what AAR monitors and why, please refer to the Information Technology Policy (Policy No. 1.07.003).

4. How we use your personal information

In addition to the purposes and uses described above, we use your personal information for the following purposes:

- To administer your relationship with us, including fulfilling any obligation that we have to provide you with compensation or benefits;
- To carry out our business effectively;
- To comply with laws or regulations to which AAR is subject;

- To comply with our contractual obligations;
- To detect and prevent fraud or crime;
- To enforce, exercise, or defend legal claims;
- To investigate potential misconduct;
- To keep your personal data and that of other staff members secure and to prevent unauthorised access, loss, damage, destruction or corruption of data. This may include monitoring communications and use of company IT equipment and systems;
- To plan, organize, and carry out administration tasks within each AAR group company and across the whole AAR group; and

Note that this privacy notice may be updated to notify you of additional purposes for which we process your personal information.

5. Sharing your personal information

In addition to the specific situations discussed elsewhere in this policy, we share your personal information in the following situations:

- **Affiliates and Business Transfers**. We may share information with our corporate affiliates (*e.g.*, parent company, sister companies, subsidiaries, joint ventures, or other companies under common control) in the course of our normal business operations. If another company acquires, or plans to acquire, our company, business, or our assets, we will also share information with that company, including at the negotiation stage.
- **Legal or Regulatory Requests and Investigations**. We may disclose information in response to subpoenas, warrants, or court orders, or in connection with any legal process, or to comply with relevant laws or regulations. We may also need to share your personal information with tax authorities, courts, regulators, the police and other governmental authorities where we are required or permitted to do so by law.
- **Other Third-Parties**. We may disclose certain information such as name, work contact details (including your workplace ID photo), training and qualification records, certifications, and other information about your work arrangements to other third parties, such as professional advisers (including lawyers, auditors and accountants), professional bodies, and regulatory authorities in the normal course of business.
- **Other Disclosures with Your Consent**. We may ask to share your information with other unaffiliated third parties who are not described elsewhere in this privacy notice.
- **Protection of AAR or Others.** We may share your information in order to establish or exercise our rights, to defend against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of person or property, or a violation of our policies.
- **Third-Party Service Providers**. We may share your information with service providers. For example, we may share your personal information with payroll administrators, pension administrators, IT service providers, training providers, benefits providers, marketing/events agencies, and recruitment agencies.

If you have any objections to the disclosures of your personal information or you would like more information about this, please contact your HR representative.

6. Data Security

We maintain reasonable physical, technical and procedural safeguards that are appropriate to the sensitivity of the personal information in question. These safeguards are designed to help protect your personal information against loss, unauthorized access or disclosure, modification, or destruction. While we use reasonable efforts to protect your personal information, we cannot guarantee the security of your personal information. In the event that we are required by law to inform you of any privacy or security event relating to your personal information we may notify you electronically, in writing, or by telephone, if permitted to do so by law.

7. Miscellaneous

The following additional information relates to our privacy practices:

- **Changes to This Privacy Policy.** We may change our privacy policy and practices over time. To the extent that our policy changes in a material way, the policy that was in place at the time that you submitted personal information to us will generally govern that information.
- **Information for California Residents.** California Civil Code 1798.115(c), 1798.130(a)(5)(c), 1798.130(c), and 1798.140 indicate that organizations should disclose whether certain categories of information are "sold" or transferred for an organization's "business purpose" as those terms are defined under California law. You can find a list of the categories of information that we share **here**. Please note that because this list is comprehensive it may refer to types of information that we share about people other than you. If you would like more information concerning the categories of personal information (if any) we share with third parties or affiliates for those parties to use for direct marketing please submit a written request to us using the information in the "Contact Information" section below.
- **Contact Information**. If you have any questions about this privacy notice, please contact a member of the Law Department. In addition, you can pose any questions your local Human Resources representative.

- **Effective Date.** This policy is effective as of September 11, 2020

.

California Information Sharing Disclosure

California Civil Code 1798.115(c), 1798.130(a)(5)(c), 1798.130(c), and 1798.140 indicates that companies should disclose whether the following categories of information are collected, transferred for consideration, or transferred for an organization's "business purpose" as that term is defined under California law. Note that while a category may be marked that does not necessarily mean that we have information in that category about you. For example, while we transfer bank account numbers for our business purpose in paying some staff members (e.g., direct deposit) we do not collect or transfer bank account numbers of staff members that do not utilize direct deposit.

Categories of Personal Information	Personal Information Collected	Collected	Disclosed for a Business Purpose	Sold
Identifiers	Name or alias	✓	✓	☐
	Contact information (such as name, address, and telephone number, e-mail address)	✓	✓	☐
	Unique Identifiers (e.g., cookies, pixel tags, device identifier and attributes, etc.)	☐	☐	☐
	Online identifiers (such as internet protocol address)	✓	✓	☐
	Government issued ID (such as social security number, driver's license number, passport number)	✓	✓	☐
Other types of Personal Information	Payment information (such as credit or debit card number)	✓	✓	☐
	Financial information (such as bank account number)	✓	✓	☐
	Medical information or health insurance information	✓	✓	☐
Characteristics of legally protected classifications	Race	✓	✓	☐
	Ethnicity	✓	✓	☐
	Gender	✓	✓	☐
Commercial Information	Information about products and services obtained from us	☐	☐	☐
	Individual's preferences	☐	☐	☐
Biometric	Fingerprint, face print, voiceprint	☐	☐	☐
	Sleep, health, exercise data	☐	☐	☐
Internet/ Electronic Activity	Browsing and/or search history	✓	✓	☐
	Information about interactions with our website, mobile application, or advertisements	☐	☐	☐
Geolocation data	Precise physical location using GPS	☐	☐	☐
Audio, electronic, visual, thermal, olfactory, or similar information	Call recordings	✓	✓	☐
	Photographs	✓	✓	☐
	Video surveillance	✓	✓	☐
Professional/employment information	Occupation	✓	✓	☐
	Employment history	✓	✓	☐
	Professional references	✓	✓	☐
Education information (ie., personally identifiable information contained in education records)	Student name	☐	☐	☐
	Name of student's parent or other family members	☐	☐	☐
	Address of student or student' family	☐	☐	☐
	Personal identifier of student (social security number, student number, biometric record)	☐	☐	☐

	Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name	☐	☐	☐
	Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty	☐	☐	☐
Inferences drawn from any of the above information		☐	☐	☐