ADCORP HOLDINGS LIMITED – PRIVACY POLICY

Process Area	Human Resources	**Policy Owner:**	Head: AHA People and Culture
Policy Title:	Privacy	**Revision No.:**	1
Policy No.:	AHA-HR-PO-017	**Next Revision Date:**	Annually

This policy is applicable to the Adcorp Group of companies, its affiliates and subsidiaries in all geographies in which it operates hereinafter referred to as "Adcorp".

Policy Summary:

The Privacy Policy outlines Adcorp's commitment to the responsible handling of personal and sensitive information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). As a recruitment and workforce solutions provider, Adcorp collects data necessary for assessing employment suitability, managing payroll, and complying with legal obligations, ensuring that sensitive information—such as health records or criminal history—is only gathered with express consent or legal authorization. The policy specifically addresses remote and hybrid work security, mandating the use of company-provided devices and secure cloud storage while maintaining transparency regarding workplace surveillance. Additionally, it integrates protections for the Right to Disconnect and safeguards against psychosocial hazards in digital environments, providing individuals with clear pathways for data access, correction, and formal complaints via the Privacy Officer or the Office of the Australian Information Commissioner (OAIC).

Approved by:

Prepared By:  Chris Bailey **Group Safety, Risk & Compliance Manager**	Date: 1st September 2025
Approved By  Laura Ford **AHA - Head of People and Culture**	Date: 1st September 2025

CONTENTS

1. POLICY STATEMENT

Adcorp is a leading recruitment company committed to connecting human potential with meaningful work. In performing our services, we collect, use, and store a variety of personal information. As a Person Conducting a Business or Undertaking (PCBU), Adcorp is dedicated to protecting the privacy of individuals whose personal information we handle, including our employees, job applicants, clients, and contractors.

This Privacy Policy outlines how Adcorp manages personal information in accordance with Australian privacy laws, ensuring transparency, accountability, and the responsible handling of data. We are committed to fostering a culture of privacy and respect for personal information.

2. SCOPE

This policy applies to all personal information collected and held by Adcorp, regardless of how it is collected or stored. This applies across both digital and physical records (e.g., hard copy forms, archived files).

It applies to:

- Employees (current and former)
- Job applicants
- Clients
- Candidates (individuals seeking employment through Adcorp)
- Contractors and service providers
- Visitors to our premises or digital platforms

3. COLLECTION OF PERSONAL INFORMATION

3.1. What is Personal Information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

3.2. What is Sensitive Information?

Sensitive information is a subset of personal information and includes information or an opinion about an individual's:

- Racial or ethnic origin
- Political opinions
- Membership of a political association
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a professional or trade association

- Membership of a trade union
- Sexual orientation or practices
- Criminal record
- Health information (including disability)
- Genetic information
- Biometric information or templates

3.3. How and Why We Collect Personal Information

Adcorp collects personal information that is reasonably necessary for, or directly related to, our business functions and activities, which primarily involve recruitment and workforce solutions. Adcorp does not collect personal information unlawfully, unfairly, or unreasonably intrusively, in line with Australian Privacy Principles 3.5

We collect information through various means, including:

Directly from you: When you apply for a job, register as a candidate, engage our services as a client, complete forms, participate in surveys, communicate with us via phone, email, or in person.

From third parties: This may include nominated referees, previous employers, educational institutions, professional bodies, publicly available sources (e.g., LinkedIn), and background check providers (with your consent where required).

Through our website and IT systems: Via cookies, analytics tools, and monitoring of company-provided devices and networks (as outlined in our Workplace Surveillance Policy).

Purposes of Collection:

We collect personal information for purposes including:

- Assessing suitability for employment or placement with clients.
- Contacting individuals regarding job opportunities.
- Managing employment relationships (for employees).
- Facilitating recruitment processes, including reference checks and background checks.
- Providing recruitment and workforce solutions to clients.
- Administering payroll, superannuation, and leave entitlements.
- Complying with legal and regulatory obligations (e.g., taxation, immigration, work health and safety).
- Managing complaints, investigations, and disciplinary matters.
- Improving our services and internal processes.
- Marketing and communication (with an opt-out option).

3.4. Collection of Sensitive Information

We only collect sensitive information when:

- It is reasonably necessary for our functions or activities (e.g., health information for fitness for work assessments, or to make reasonable adjustments for a disability).
- You have given your express consent.
- It is required or authorised by law (e.g., criminal history checks for specific roles).

4. USE AND DISCLOSURE OF PERSONAL INFORMATION

Adcorp uses and discloses personal information for the primary purpose for which it was collected, or for a secondary purpose where:

- You have consented to the use or disclosure.
- You would reasonably expect us to use or disclose the information for the secondary purpose, and that purpose is related to the primary purpose (or directly related for sensitive information).
- It is required or authorised by or under an Australian law or a court/tribunal order.
- It is necessary to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety.

Where personal information is disclosed to overseas service providers (e.g., cloud storage providers), Adcorp takes reasonable steps to ensure the recipient does not breach the Australian Privacy Principles.

Disclosure to Third Parties:

We may disclose personal information to:

- Our clients (for candidate placements, with your consent).
- Referees (with your consent).
- Service providers (e.g., IT support, payroll providers, background check agencies, superannuation funds, insurers).
- Government agencies or regulatory bodies (where required or authorised by law).
- Professional advisors (e.g., lawyers, accountants).
- Other third parties with your consent or as permitted by law.

We take reasonable steps to ensure that third parties to whom we disclose personal information are bound by appropriate privacy and confidentiality obligations.

5. DATA QUALITY AND SECURITY

Adcorp takes reasonable steps to ensure that the personal information we collect, use, and disclose is accurate, up-to-date, complete, and relevant. We also take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure. In the event of a data breach involving personal information, Adcorp will respond in accordance with its Data Breach Response Plan and may notify affected individuals and the Office of the Australian Information Commissioner (OAIC), where required by law.

Our security measures include:

- Physical security of our office premises.
- Secure electronic databases and information systems.
- Access controls and authentication for IT systems.

- Encryption of sensitive data where appropriate.
- Regular security assessments and updates.
- Employee training on privacy and data security.

When personal information is no longer needed for the purpose for which it was collected, and we are not legally required to retain it, we take reasonable steps to destroy or de-identify it.

6. ACCESS AND CORRECTION

You have a right to request access to the personal information Adcorp holds about you and to request that it be corrected if it is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

To request access or correction, please contact our Privacy Officer (details below). We will respond to your request within a reasonable time and, where possible, provide access or make the correction. We may charge a reasonable fee for providing access, but not for making a correction.

In certain circumstances, we may refuse access or correction, in which case we will provide written reasons.

7. WORKING FROM HOME AND REMOTE WORK CONSIDERATIONS

As Adcorp supports remote and hybrid work arrangements, specific privacy and IT security considerations apply:

7.1. IT Aspects and Data Security for Remote Work

- **Company Devices:** Employees working remotely must use company-provided devices (laptops, phones) for all work-related activities. Personal devices should not be used for Adcorp business.
- **Secure Networks:** Employees must ensure they work on secure, password-protected networks. Public Wi-Fi networks should be avoided for sensitive work.
- **Physical Security:** Remote employees are responsible for the physical security of company devices and confidential information within their home environment, ensuring it is not accessible to unauthorised individuals (e.g., family members, housemates).
- **Software and Updates:** All company devices must have up-to-date operating systems, antivirus software, and security patches. Employees must not install unauthorised software on company devices.
- **Data Storage:** All work-related data must be stored on Adcorp's approved cloud storage or network drives, not on local device storage.
- **Monitoring:** As outlined in our Workplace Surveillance Policy, Adcorp may monitor the use of company-provided computers and networks to ensure compliance with company policies, protect company assets, and maintain system integrity. This monitoring is conducted transparently and in accordance with legal requirements.

Employees should report any suspected breaches (e.g., stolen devices, unauthorised access).

7.2. Right to Disconnect

Adcorp recognises the importance of work-life balance and the "right to disconnect" for its employees. This right allows employees to refuse to monitor, read, or respond to contact (or attempted contact) from the employer or a third party outside their working hours, unless doing so is unreasonable.

When determining if a refusal is unreasonable, Adcorp will consider factors such as:

The reason for the contact (e.g., genuine emergency, critical business need).

- How the contact is made and its disruptiveness.
- Any compensation or payment for being available outside ordinary hours.
- The employee's role and level of responsibility.
- The employee's personal circumstances (e.g., family or caring responsibilities).
- Any expectations clearly communicated and agreed upon in the employment contract or relevant industrial instrument for specific roles (e.g., on-call duties).
- Adcorp encourages open communication between managers and employees regarding expectations for out-of-hours contact. Employees will not be penalised for reasonably exercising their right to disconnect.

7.3. Psychosocial and Gender-Based Harassment in Remote Environments

Adcorp is committed to providing a workplace free from psychosocial hazards and all forms of harassment, including gender-based harassment, regardless of whether work is performed in the office or remotely.

- **Reporting:** Employees are encouraged to report any incidents of psychosocial hazards or harassment, including those occurring in remote work settings (e.g., via online communication platforms). All reports will be handled sensitively and confidentially, with due regard for the privacy of all parties involved.
- **Investigations:** Investigations into harassment complaints will be conducted fairly, impartially, and with a trauma-informed approach, ensuring the privacy and emotional safety of affected employees. Information collected during investigations will be kept confidential and only disclosed on a need-to-know basis or as required by law.
- **Training:** Adcorp provides training to employees and managers on identifying and preventing psychosocial hazards and harassment, including specific guidance for remote work interactions.

8. COMPLAINTS AND BREACHES

If you believe Adcorp has breached its privacy obligations or this Privacy Policy, please contact our Privacy Officer in writing. We will investigate your complaint and respond to you within a reasonable timeframe.

If you are not satisfied with our response, you may escalate your complaint to the Office of the Australian Information Commissioner (OAIC).

9. CONTACT US

If you have any questions about this Privacy Policy or Adcorp's privacy practices, please contact our Privacy Officer:

Privacy Officer

Adcorp

Level 8, 210 George Street, Sydney, NSW, 2000

Email: privacy@adcorpaistralia.com.au

Phone: 1300 268986

10. POLICY REVIEW

This policy will be reviewed periodically or as required, to ensure its ongoing effectiveness and compliance with legislative changes.

11. DOCUMENT HISTORY

The following table lists the changes made to this document:

Version	Date	Author	Change
1.0	1/09/2025	C.Bailey	Original document

ANNEXURE A – RELATED DOCUMENTATION AND LEGISLATION

This policy should be read in conjunction with the following legislation and other Adcorp policies and documentation:

Australia:

Legislation applicable to Australia:

Privacy Act 1988 (Cth): The cornerstone of Australian privacy law, including the Australian Privacy Principles (APPs).

Fair Work Act 2009 (Cth): Regulates workplace relations, including general protections, unfair dismissal, and the "right to disconnect" provisions.

Work Health and Safety Act 2011 (Cth): Sets out the primary duty of care for PCBUs regarding health and safety, including psychosocial hazards.

Disability Discrimination Act 1992 (Cth): Prohibits discrimination on the basis of disability and mandates reasonable adjustments.

Sex Discrimination Act 1984 (Cth): Prohibits discrimination and sexual harassment on the basis of sex, sexual orientation, gender identity, and intersex status.

Telecommunications (Interception and Access) Act 1979 (Cth): Regulates the interception of communications.

State and Territory Legislation

Work Health and Safety (WHS) Acts (and associated Regulations):

New South Wales: Work Health and Safety Act 2011 (NSW)

Victoria: Occupational Health and Safety Act 2004 (Vic)

Queensland: Work Health and Safety Act 2011 (Qld)

Western Australia: Occupational Safety and Health Act 1984 (WA)

South Australia: Work Health and Safety Act 2012 (SA)

Tasmania: Work Health and Safety Act 2012 (Tas)

Australian Capital Territory: Work Health and Safety Act 2011 (ACT)

Northern Territory: Work Health and Safety (National Uniform Legislation) Act 2011 (NT)

Anti-Discrimination / Equal Opportunity Acts:

New South Wales: Anti-Discrimination Act 1977 (NSW)

Victoria: Equal Opportunity Act 2010 (Vic)

Queensland: Anti-Discrimination Act 1991 (Qld)

Western Australia: Equal Opportunity Act 1984 (WA)

South Australia: Equal Opportunity Act 1984 (SA)

Tasmania: Anti-Discrimination Act 1998 (Tas)

Australian Capital Territory: Discrimination Act 1991 (ACT)

Northern Territory: Anti-Discrimination Act 1992 (NT)

Surveillance Devices / Workplace Surveillance Acts:

New South Wales: Workplace Surveillance Act 2005 (NSW); Crimes (Surveillance Devices) Act 2005 (NSW)

Victoria: Surveillance Devices Act 1999 (Vic)

Queensland: Invasion of Privacy Act 1971 (Qld) (primarily covers listening devices); Work Health and Safety Act 2011 (Qld) may also be relevant for workplace monitoring.

Western Australia: Surveillance Devices Act 1998 (WA)

South Australia: Surveillance Devices Act 2016 (SA)

Tasmania: Listening Devices Act 1991 (Tas)

Australian Capital Territory: Workplace Privacy Act 2011 (ACT); Surveillance Devices Act 2007 (ACT)

Northern Territory: Surveillance Devices Act 2007 (NT)