

## Barringtons Privacy Policy

Barrington Group Australia Pty Limited (Barringtons) – inclusive of Barrington Corporate Risk Pty Limited, Barrington Personnel Security, Barrington Training Services Pty Limited and Barringtons Smartek – respects the rights of its clients and staff and is committed to complying with all applicable privacy and confidentiality legislation.

### SCOPE AND PURPOSE

This policy applies to all Barringtons' staff (i.e. its employees, contractors and students).

This policy has been developed to provide a framework for Barringtons legal and ethical expectations in dealing with confidentiality and privacy matters.

### DEFINITIONS

#### **Personal Information (defined by the *Privacy Act 1988*)**

**Personal information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in a material form or not.

#### **Sensitive Information (defined by the *Privacy Act 1988*)**

**Sensitive information** means:

- (a) information or an opinion about an individual's:
  - (i) racial or ethnic origin; or
  - (ii) political opinions; or
  - (iii) membership of a political association; or
  - (iv) religious beliefs or affiliations; or
  - (v) philosophical beliefs; or
  - (vi) membership of a professional or trade association; or
  - (vii) membership of a trade union; or
  - (viii) sexual orientation or practices; or
  - (ix) criminal record;

that is also personal information; or

- (b) health information about an individual; or
- (c) genetic information about an individual that is not otherwise health information; or
- (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- (e) biometric templates.

### CONFIDENTIALITY

Implies the relationship of confidence between Barringtons, its staff and its clients.

## GENERAL MATTERS

We recognise the rights of clients and Barringtons staff to maintain their privacy and confidentiality and to have their information administered in ways which they would reasonably expect.

As a 'contracted service provider' in both the Commonwealth and state jurisdictions, where a service agreement exists:

- in the Commonwealth jurisdiction (as a contract between a Commonwealth Government agency and Barringtons), the *Privacy Act 1988* ([The Privacy Act | OAIC](#)) and the Australian Privacy Principles (APPs) ([The Australian Privacy Principles \(oaic.gov.au\)](#)) will prevail and apply, or
- in the state jurisdiction (as a contract between a state government agency and Barringtons) the *Information Privacy Act 2009* will prevail and apply.

Every Barringtons staff member will receive training in awareness of the privacy principles and this policy. Staff of Barrington Personnel Security undertaking work for the Australian Government Vetting Agency should also be familiar with the *Defence Privacy Policy* (see: [Privacy Policy | About | Defence](#)).

Dignity and privacy will also be extended to clients when they visit our premises with the provision of private meeting rooms to undertake confidential discussions, when it is applicable and available to do so.

It is a criminal offence for any individual to falsify records and any Barringtons staff member who is aware of this occurring is to report it immediately to their supervisor or senior management.

## COLLECTION, USE AND DISCLOSURE OF INFORMATION

Barringtons collects personal information when it's reasonably necessary for, or directly related to, our functions or activities.

Barringtons may also collect sensitive information where collection is allowed under the Privacy Act (e.g. where you consent).

Barringtons collects the information for the purpose of delivering direct services, administering processes associated with service delivery e.g. vetting, referrals, meeting any requirements for government funding, monitoring or evaluating the services we provide, to comply with legal obligations or to produce annual reports or for research purposes. Barringtons also collects personal information from employees for the purpose of administering their employment conditions. The nature and extent of the information collected by Barringtons varies depending on the individual's interaction with us.

Such information may include:

- Contact details (name, address, email, etc.)
- Personal details (date of birth, gender, income, emergency contacts, etc.)
- Information to verify your identity (e.g. tax file numbers, biometric information).
- Criminal history
- Information about your circumstances (e.g. family circumstances, financial situation, employment, health and welfare)
- Australian Business Number (ABN)
- Server address and online visit information.

As part of the vetting process, Barrington employees and subcontractors collect, hold, use, and disclose personal information from clearance subjects, referees, or third parties to assess an individual's suitability for accessing government information. Subcontractors engaged for specific tasks, such as vetting, undergo the same background checks as employees and are bound by strict service agreements to ensure compliance with regulatory requirements.

This information may be collected by Barringtons using in-person interviews, registrations or application processes, online or electronic registration or communications, questionnaires or over the telephone. Any individual who accesses external links via our website will need to check that particular website's privacy policy.

If clients would like to access any Barringtons services on an anonymous basis or using pseudonym, the client is required to advise us and, if it is possible and lawful, we will take all reasonable steps to comply with the request. However, Barringtons may not be able to provide the services in question if we are not provided with the personal information requested.

Barringtons only uses personal and sensitive information for the purposes for which it was given to us, or for purposes which are relation to one of our services. We may also disclose information, consistent with the Privacy Act, to other external organisations such as funding bodies, contractors who work for us, other regulatory bodies, referees or our professional advisors including our accountants, auditors and solicitors.

Any personal details collected will not be disclosed to any other person or agency external to Barringtons without the individual's written consent or unless required or authorised by law. If we receive information about an individual from a third party, Barringtons will take all reasonable steps to contact that individual to ensure that you are aware of the purposes for which we are collecting that information.

Barringtons retains personal information only for as long as it is required for the purposes it was collected. After this period, information is securely destroyed or archived in compliance with regulatory requirements.

It should be noted that 'use' and 'disclosure' are separate practices, with 'use' being the handling or management of information within Barringtons, whereas 'disclosure' is when information is released from our control to another individual or entity.

In relation to information collected by Barrington Personnel Security undertaking work for the Australian Government Security Vetting Agency (AGSVA), it should be noted that the Department of Defence retains control over all this information.

As part of its contractual obligations to AGSVA, Barrington Personnel Security is required to:

- meet privacy requirements (such as compliance with the APPs, information security, training, and auditing)
- advise AGSVA if they become aware of any potential breach of those obligations, and
- in relation to personal information obtained, advise AGSVA of:
  - any disclosure of that personal information required by law, or
  - any approach by the Privacy Commissioner or the individual to whom the personal information relates.

### **EXEMPTIONS FOR DISCLOSURE**

Generally, Barringtons will use and disclose your personal information for the same purpose as collected. Barringtons may use and disclose your personal information for a secondary purpose if you consent or another provision in the Privacy Act allows it.

Situations where this may occur include the following:

- Where there is serious risk of abuse or physical harm to the individual or other person, including our clients, the general public and own staff members
- Where the disclosure is required under a law
- Where the individual would reasonably expect us to use or give that information, e.g. Referral processes
- When the disclosure is necessary by or for a law enforcement agency (e.g. Prevention, investigation, prosecution or punishment of criminal offences, protection of public revenue, preparation or implementation of a court or tribunal order.)

In the event that a legal need for disclosure arises, the staff member will inform their supervisor or manager prior to making the decision to breach confidentiality and privacy. This decision will also be communicated to the individual, unless such advice to the individual is not allowed by legislation.

### **INFORMATION SECURITY**

Barringtons ensures that safeguards are in place to protect the personal information it administers against loss, interference, unauthorised access, inappropriate disclosure, modification or other misuse. These safeguards include reasonable physical and technical steps for both electronic and hard copy records. Some of these include, but are not limited to:

- Securing information in lockable storage cabinets
- Not storing personal information in public areas
- Restricting physical access
- Positioning electronic equipment so that they cannot be seen or accessed by unauthorised persons, and/or
- Using passwords, different levels of information systems access, anti-viral software and firewalls to restrict unauthorised use.
- Storing personal information on secure IT systems with restricted access based on staff permissions

Access logs are monitored, and periodic audits are conducted to ensure compliance. Upon employee termination, access is immediately revoked as part of our off-boarding procedures. Hard copies of personal information are securely stored and destroyed once no longer required.

Access to personal information about an individual is restricted to Barringtons staff who have a need to access the information for purposes which are directly related to or reasonably necessary for their duties.

The Code of Conduct also outlines the expectations of Barringtons staff to take all reasonable steps to protect organisational and personal information and all staff and third party contractors are required to sign a confidentiality and privacy agreement to that effect.

### **INFORMATION QUALITY AND ALTERATIONS**

Barringtons takes steps to ensure that information that it collects is accurate, up-to-date and complete. These steps may include maintaining and updating information either proactively or when we are advised by individuals that the information has changed, and can include checking information that is provided by a person about another individual is correct.

Should any information be deemed to be inaccurate or require deletion, the individual can discuss the required amendments with the Privacy Officer at [melissa.francis@barringtongroup.com.au](mailto:melissa.francis@barringtongroup.com.au).

In the event that the Privacy Officer declines the request to have information amended, the individual has the right to lodge an appeal of this decision with the Chief Executive Officer using the [Feedback and Complaint Management Policy](#) and associated procedure.

### **ACCESS TO AND CORRECTION OF PERSONAL INFORMATION**

Individuals have a right to request:

- access to personal information that Barringtons hold about them
- correction to the personal information Barringtons hold about them

Barringtons will provide an individual access to the personal information held about them in the manner requested if it is reasonable and practicable to do so.

Barringtons will also take reasonable steps to correct personal information held about an individual if we consider it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If we refuse to provide an individual with access to, or to correct, their personal information, Barringtons will notify the individual in writing and explain the reasons.

Requests should be directed to Barrington's Privacy Officer at [melissa.francis@barringtongroup.com.au](mailto:melissa.francis@barringtongroup.com.au). Requests will be processed within 30 days in accordance with the Privacy Act.

### **COMPLAINTS ABOUT BREACHS OF THE APPs**

If a Barringtons staff member is dissatisfied with the conduct of a colleague regarding privacy and confidentiality of information, the matter should be raised with the staff member's direct supervisor. If this is not possible or appropriate, follow the steps indicated in the [Grievance Policy](#). Staff members who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action. A staff member's obligation with respect to confidentiality survives the termination of their employment with Barringtons.

If a user of Barringtons' services is dissatisfied with the conduct of one or more of our staff members regarding privacy and confidentiality of information, the client is encouraged to lodge a complaint via the [Barrington's Privacy Complaint Form](#) to address their concerns. Alternatively the client can contact the Barrington's Privacy Officer on [melissa.francis@barringtongroup.com.au](mailto:melissa.francis@barringtongroup.com.au).

Our process is designed to ensure that all privacy concerns are managed promptly, thoroughly, and in accordance with Barringtons' commitment to privacy. The following steps outline our approach:

- Upon receiving your complaint, Barringtons will confirm receipt within 3 business days.
- Barringtons will investigate your complaint thoroughly, including reviewing the circumstances and speaking with relevant staff or stakeholders as necessary.
- A formal resolution or response will be provided to you within 14 business days of acknowledging your complaint.

Should the individual not be satisfied with the complaint management, they can report their concern to the Office of Australian Information Commissioner.

See [What you can complain about | OAIC](#)

**ACCESSIBILITY REQUIREMENTS (WCAG Compliance)**

This Privacy Policy is compliant with WCAG A/AA standards, ensuring accessibility for all individuals, including those using assistive technologies. The policy is available on [Barrington's website](#). For alternative formats, please contact us via [melissa.francis@barringtongroup.com.au](mailto:melissa.francis@barringtongroup.com.au).