
PRIVACY POLICY

Context and purpose

This policy has been developed to ensure the Company complies with The National Privacy Principles (NPP) in the *Privacy Act 1988 (Cth)* (**the Act**) which apply to Private Sector organisations.

Whilst employee records are exempt from compliance with the NPP, documents that do not fall within the definition of “Employee Records” as outlined below and information relating to contractors and unsuccessful job applicants are governed by the NPP.

Policy

This policy applies to all personal information collected by the Company relating to individuals including:

- all current and former employees of the Company where the information is not held in Employee Records or its use and disclosure does not relate to the employment relationship;
- applicants for employment who were unsuccessful in securing employment with the Company (as documents relating to successful job applicants that become employees also become “Employee Records”); and
- contractors.

Personal Information is defined in the Act as information about an individual who can be identified, or whose identity could be reasonably ascertained, from the information.

This policy does not apply to Employee Records which are defined in the Act as records of personal information relating to the employment of an employee.

Examples of personal information relating to the employment of an employee include health information about the employee and personal information about all or any of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;
- the employee's membership of a professional or trade association;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and
- the employee's taxation, banking or superannuation affairs.

Collection of personal information

Personal information collected and/or maintained by the Company must be relevant to the purpose for which it is sought, must be accurate, up-to-date and complete, and must not intrude to an unreasonable extent upon the personal affairs of the individual to whom it relates.

This information must be obtained, maintained and managed fairly and with respect for the dignity of the individual to which it relates. Individuals providing information should be advised of the general purpose for which the information is sought, and how it may be used in the future.

At the same time, information supplied by individuals is expected to be, to the best of their knowledge, true and accurate.

Use and disclosure of personal information

The Company will not use or disclose personal information about an individual for a purpose other than the purpose for which that information was collected or a secondary purpose which the individual would reasonably expect the information to be used for. In particular, the Company must not sell or otherwise provide unauthorised access to such information to anyone.

The only exceptions to the above are where:

- the information is request by a government department / authority or solicited as evidence in court;
- the Company has permission from the individual to disclose such information; or
- the individual's health, safety or general well-being may be reasonably thought to be at risk by non-disclosure.

Organisations seeking confirmation of employment or other personal information about a current or former employee are required to fax, mail or email their request on their organisation's letterhead, to the Company and must send a copy of that request to the employee concerned and obtain their permission to release information.

Storage of personal information

For practical reasons, personal information will be maintained and will form part of Human Resources' secure record system.

Any person responsible for the maintenance or use of personal information must ensure that the information is adequately protected against:

- loss;
- damage; or
- unauthorised use, modification, or disclosure.

Openness about personal information

On request by an individual, the Company will take reasonable steps to let an individual know generally:

- what sort of personal information it holds about the individual;
- for what purposes; and
- how it collects, holds, uses and discloses the information.

Access to personal information

Subject to reasonable requests, individuals will have access to review personal records relating to them, except where:

- providing access would have an unreasonable impact upon the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the Company and the individual and the information would not be accessible by their process of discovery in those proceedings;
- providing access would prejudice the Company in relation to negotiations with the individual;
- providing access would be unlawful;
- denying access is required or authorised by law; or
- providing access would be likely to prejudice an investigation of possible unlawful activity.

Where for any reason the Company denies access to information, it will provide reasons for the denial.

Correction of personal information

If an individual establishes to the Company that personal information held by the Company about the individual is not accurate, complete and up to date, the Company will take reasonable steps to correct the information so that it is accurate, complete and up to date.

If for some reason the Company and individual disagree about whether the information is accurate, complete and up to date, the Company will, upon request by an individual, take reasonable steps to associate with the information a statement from the individual claiming that the information is not accurate, complete or up to date.

Sensitive information

“Sensitive Information” is health information or personal information or an opinion about an individual’s:

- racial or ethnic origin; or
- political opinions; or
- membership of a political association; or
- religious beliefs or affiliations; or
- philosophical beliefs; or

- membership of a professional or trade association; or
- membership of a trade union; or
- sexual preferences or practices; or
- criminal record;

The Company will not collect Sensitive Information about an individual unless:

- the individual has consented; or
- the collection is required by law; or
- the collection is necessary to prevent or lessen a serious and imminent threat to the life of any individual, where the individual whom the information concerns is physically or legally incapable of consenting to the collection; or physically cannot communicate to consent to the collection; or
- the information is necessary to provide a health service to the individual and the information is collected:
 - as required by law; or
 - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality that bind the Company.

Information relating to applicants

All applicants will be informed of the existence of this policy and offered a copy of this policy as soon as reasonably practicable after their application is received by the Company.

Application forms, test results, medical reports, records of interview and other relevant information relating to unsuccessful job applicants will be retained by the Company for a minimum of one month but no longer than six months, unless the applicant requests (in writing) that the information be destroyed earlier or kept for longer.

Unsuccessful applicants for positions with the Company may request the return of material supplied by them in support of their application. They will also be able to request access to information collected during the employment process.

Except as may be required as part of the debriefing process relating to unsuccessful internal applicants, no information will be conveyed, either verbally or in writing, to any person not directly involved in the employment process about any applicant for the position.

The Company will not contact an applicant's previous employers without the permission of the applicant, however inclusion by the applicant of referees in the application and/or their resume will be regarded as permission to contact such referees.

Request from other employers

Where a person has listed the Company as a previous or current employer, the Company will only, with the consent of the former employee, supply information relating to the period of employment and type of work the employee performed.

When requested by the former employee, Human Resources will issue a Statement of Service on the Company's letterhead. Only the employee's name, role, department or

section, commencement date, termination date, and reason for termination of employment will be documented in the Statement of Service.

All employment checks must be first directed to Human Resources. Only Human Resources or the Managing Director are authorised to provide this information on behalf of the Company.

It is against this policy for any employee of the Company to give a written or verbal reference outside the scope of what has been outlined above. If, for any reason, a manager, supervisor or any other employee of the Company is contacted by a prospective employer or any other third party to act as a referee for a current or former employee (or by a financial institution to check credit ratings of current or former employees), it is against this policy to provide any information other than to confirm the information contained on the Statement of Service as outlined above.

If any employee does not adhere to the Company's policy and proceeds to provide any such reference, the employee's actions will not bind the Company and the employee will be personally liable for any misrepresentations or damage suffered by a prospective employer or third party in respect of that reference or any misrepresentations or damage resulting from that reference. Disciplinary action may also occur.

Method of disposal

All personal information must be disposed of in a manner that ensures the privacy of the individual to whom it relates. Destruction will usually be by means of shredding, burning, or secure disposal by registered waste contractors.

Compliance and complaints

Employees and Contractors must comply with this policy. If an employee fails to comply with these policies, they may be subject to disciplinary action, up to and including termination of their employment. If a contractor fails to comply with this policy, their contract may be terminated without notice.

The Company has a complaints handling process in place to manage privacy risks and issues. This process is designed to:

- identify and address any request for information or complaints;
- increase consumer confidence in the Company's privacy procedures; and
- help build and preserve the Company's reputation and business.

Any employee, contractor or relevant third party that knows about or suspects a privacy breach must immediately report to management.

- Variations to the above policy guidelines will only be approved under special circumstances by the Regional Manager or Group Finance Manager in conjunction with the General Manager or Managing Director.
- Any questions in relation to this policy should be directed to the Personal Assistant to the General Manager.