Privacy Policy

The objective of this policy is to set guidelines for the collection, use, access, correction, deletion, and storage of personal information that complies with the National Privacy Principles (NPP's).

The company recognises that it is both necessary and required by law for the company to hold records of a variety of factual information about employees and prospective employees in order for necessary daily running of the company.

The company accepts that the general principles of confidentiality and privacy apply to the use and availability of its records. Where information about a person includes personal details as defined by the Privacy Act 1988 as amended, that person may quite reasonably expect that the company will maintain confidentiality, except where disclosure is required for legitimate and legal purposes.

Key Points

1. The company collects, maintains, utilises and discloses personal information covered by the privacy legislation.

The information collected by the company includes:

a) Personal information on prospective employees.
b) Sensitive information on psychometric testing candidates.
c) Personal information on client contacts and prospective client contracts including business relationship history.
d) Personal information on supplier contacts.

2. This private information is primarily stored on both secure databases and in hard copy form that is only accessible to authorised employees with a genuine need to access the information as part of their employment.
3. Unless required by law or permitted by consent, the information collected by the company is not used for any purpose other than the primary purpose for which it was collected, or a related and reasonably foreseeable secondary purpose.
4. The company will endeavour to ensure that all employees, contractors, agents and other people working within the company are familiar with this policy and other appropriate guidelines.

Definitions

Personal Information:

Personal information is broadly defined as any information or opinion that can identify a person.

Sensitive Information:

Sensitive information is defined as any combination of the following:

- Racial/ethnic origin
- Membership of union

- Political opinions
- Professional or trade associations
- Political association
- Sexual preferences or practices
- Religious beliefs or affiliations
- Criminal record
- Philosophical beliefs
- Health information

Authorised Access to Records:

The company defines authorised access to that which is required from work-related purposes. For example, reaching selection decisions or providing vocational guidance.

Procedures

NPP1: Collection of Personal Information

The company will only collect personal information where the information is necessary for one or more of its functions or activities. The company will collect this information in a way that is fair, lawful and not intrusive.

It is the company's responsibility to take reasonable steps to ensure that the person providing the information is made aware of:

a) The name of the organisation collecting the information.
b) How to contact the organisation collecting the information.
c) The fact that the person can gain access to the information.
d) The purpose of the collection.
e) The organisations (or types of organisations) to which the organisation usually discloses information of that kind.
f) What happens, if anything, if the person does not give any or all of the information.

Where information about an individual is collected from a third party, the company will take reasonable steps to notify the individual of the above information.

These obligations will be met through the use of appropriate forms and training of staff.

NPP2: Use and Disclosure

The company will only used or disclose information for the following reasons:

The purposes it was collected (unless the person has consented).
If the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure.
Direct marketing in specified circumstances.
In circumstance related to public interest such as law enforcement and public health.

The company will endeavour to receive an individual's consent for disclosure of his/her information by way of writing. If necessary, verbal consent will be accepted and a file note or database record will be taken.

NPP 3: Data Quality

The company will take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

The company will endeavour to do this by filling out a "change of details" form when a change is required to be made to the information. This change of details form must be submitted to the data controller as soon as possible and is to be corrected within two working days.

NPP 4: Data Storage

Reasonable steps will be taken to protect personal information from misuse, loss and unauthorised access modification or disclosure.

Reasonable steps will be taken to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed.

The following process will be implemented:

- No personal information should be given over the phone unless it has been established that the caller has legitimate grounds to access the information and given proof of identify.
- No personal information should be left on voicemail unless requested by the owner of the voicemail on the basis that the voicemail is secure.
- Mail containing personal information should be labelled "Private and Confidential: Attention…"
- Fax machines used for transmission of personal health information should be secure.
- Only authorised individuals should receive personal information and are not permitted to forward such information without consent.
- Paper records containing personal information should not be copied unless it is essential to do so.
- All paper records should be kept in lockable storage when not in use and should be shredded or burned when no longer required.
- The anonymity of client contacts should be maintained during presentations, consultation with other clients, suppliers and other members of the public, research activities and public events.
- Personal information should not be left unattended nor should it be discussed in public areas where others may overhear.
- Employees and other persons who are directly involved with the activities of the company are required to consent to applicable confidentiality obligations in writing.

NPP 5: Openness

This policy will be made available to anyone who asks for it and will be reviewed/modified where appropriate in order for information systems to run smoothly.

On request by a person, the company will take reasonable steps to let the person know what sort of personal information it holds, for what purposes it is held and disclosed. Any such requests are to be directed to the Chief Executive Officer or the Administration Manager.

NPP 6: Access and Correction

The company acknowledges that it must give an individual access to their personal information on request. This is limited by a number of things.

For example:

- In the case where it would pose a threat to the life of any individual.
- Where the request for access is frivolous or vexations.
- Where denying access is required or authorised by or under law.
- Where providing access would reveal evaluative information generated within the company, in connection with a commercially sensitive decision-making process, the company may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
- If the individual is able to establish that the information is not accurate, complete or up-to-date, the company will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.
- Where an individual and the company disagree about whether the information is accurate, complete and up-to-date, and individual asks the company to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the company will take reasonable steps to do so.
- The company will provide reasons for a denial of access or a refusal to correct personal information.

All inquiries regarding access or correction in accordance with this policy must be communicated to the Chief Executive Officer or the Administration Manager.

NPP 7: Identifiers

Generally, the company will not adapt, use or disclose, an identifier that has been assigned by a Commonwealth Government agency. In most cases, personal information will be stored by the person's last name or the associated organisation.

NPP 8: Anonymity

Where it is lawful and practicable to do so, individuals will have the option of not identifying themselves when entering transactions with the company.

NPP 9: Transborder Data Flows

The company does not generally transmit information overseas, however, in such an unlikely event, the company will only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

NPP 10: Sensitive Information

Sensitive information will not be collected unless:

- The individual has consented.
- It is required by law.
- The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the subject of the information is physically or legally incapable of giving consent.
- The collection is necessary for the establishment, exercise or defence of a legal claim.

Complaints

Complaints about breaches of personal privacy should be reported to the company's Chief Executive Officer.