Employee Privacy Policy

Policy Statement

The company is committed to protecting the privacy of its employees in all areas, but particularly in the collection, security, use and disclosure of their personal information.

The company complies with privacy laws and the Australian Privacy Principles contained in the Privacy Act 1988 (Cth) (the Privacy Act) which sets out the standards, rights and obligations in relation to handling, holding, accessing and correcting personal information and prohibits the disclosure of personal information subject to a limited number of exemptions.

The company acknowledges the particular importance of this policy in relation to Human Resources and Payroll as information collected may be of a sensitive nature.

Policy Application

This Policy applies to all personal information relating to potential, current and past employees and contractors of the company.

Definitions

Personal Information is legally defined as: 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. Individual means a natural person and does not include deceased persons.

Sensitive Information is legally defined as any information about a person's racial or ethnic origin, political opinion, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information.

Australian Privacy Principles and Employee Records relates to the handling of an employee's personal information by a private sector employer being exempt for the Privacy Act if it is directly related to an employee's current or former employment relationship or an employee record related to the employee. This means that an employer does not have to grant an employee access to the employee's employee records under the Privacy Act.

Collection of Personal and/or Sensitive Information

Personal information will only be collected for a lawful purpose that relates to company work and where the collection of the information is necessary for, or directly related to, that purpose. It must be obtained lawfully and fairly.

The company generally collects personal information directly from employees and applicants but may also collect personal information from an employee's supervisors, other employees or intermediaries such as recruitment agents and personnel providers.

The company may also collect personal information about employees and applicants from third parties, for example previous employers, when it is relevant to the selection process. Personal Information may also be collected through various means including but not limited to interviews, correspondence, by telephone and/or email, via websites and social media, from media and publications, from other publicly available sources etc.

Sensitive information will only be collected by the company

- for the primary purpose for which it was obtained
- for a secondary purpose that is directly related to the primary purpose
- with the consent of the employee; or where required or authorised by law.

In rare cases the company may collect sensitive information without employees consent such as where it is necessary to investigate suspected unlawful activity or misconduct of a serious nature within our organisation.

Storage and Security of Personal Information

The company will take reasonable steps to protect the personal information held from misuse, loss and from unauthorised access, modification or disclosure. Personal information that is no longer required will be destroyed or, where appropriate, de-identified.

We may store information either physically or electronically in the following ways:

- On Flare, the Payroll System, Payroll and Finance related databases which are housed both onsite and offsite and accessible only by authorised personnel and;
- Hard copy employee files which are housed offsite in secure methods, including lockable storage with access available only to authorised personnel.

Electronic records shall only be accessible to employees who have been issued with a personal login identification and access by Business Technology. Employees will only be given a level of access appropriate to their duties.

Paper records will be housed in areas restricted to Human Resources and Payroll staff, or employees accompanied by Human Resources or Payroll staff. If these areas are unattended they will be locked.

The company will only store personal information for as long as necessary for the purpose for which the information was sourced and provided and / or as required by law. In such cases, the company will take reasonable steps to destroy or permanently de-identify an employee's Personal Information.

The company will store interview notes taken throughout the recruitment process in line with the company Recruitment policy.

In addition, the company will provide requests for employee information when directed under law or to authorities who are approve to access such information. For example; Fair Work Inspectors and organisation officials (such as a trade union) may access employee records (including personal information) to determine if there has been a contravention of relevant Commonwealth workplace laws.

Information Collected for and/or Contained within an Employee's Personal File

Human resources files hold personal information such as yet not limited to:

- employee, referee and emergency contact details
- applications for employment and supporting documents
- selection reports
- pre-employment checks including but not limited to police checks, bankruptcy checks, ASIC Banned and Disqualified checks etc
- employment contracts, and other records relating to terms and conditions of employment
- transfer of Business records
- details of financial and other personal interests supplied by employees and their immediate family members for the purpose of managing perceived or potential conflicts of interest
- proof of Australian citizenship
- certified copies of academic qualifications
- records relating to salary, employment benefits and leave
- medical certificates or health related information supplied by an employee or their medical practitioner including information about pre-existing illnesses or injuries
- taxation details
- banking information necessary to pay salary and wages
- superannuation contributions
- information relating to employees' training and development
- information relating to an employee's termination
- information about an employee's performance.
- Workers compensation claims, files and correspondence (in the event there is not a dedicated Workers Compensation Specialist in the company that can quarantine those files)

Employee's Right to Restricted Access to Personal Information and Employment Records

An Employee does not have a general right to access and review their employment records however they do have a right to access and update or correct their personal information, subject to some exceptions allowed by law. Information in an employment record that an employee is able to view includes:

- award which governs employment
- time and wages records including overtime and remuneration

- records of leave, including leave taken and available entitlements
- records of superannuation contributions; and
- workers compensation payment records, if an employee has had an accident.

An Employee cannot look at another employee's employment record except if their duties expressly require it (e.g. an HR manager, payroll officer and similar roles).

If an employee wishes to access their records they must submit a request in writing to the Head of HR indicating the reason access to the record is being sought. The company must respond to the request within 30 calendar days commencing the day after the request is received.

If that timeline is impracticable the company will contact the individual to explain the delay and provide an expected timeframe.

The Head of HR, or a Payroll Officer or Manager if nominated by the Head of HR, will allow employees to so inspect the approved/relevant records in their presence. Records may not be removed from the secure area but employees may generally be given copies of approved records they request. Any identifying information about another person must be de-identified before being provided.

Employees may authorise or consent to an organisation or another person having access to their personal information. The law allows for either direct consent (written or, if time does not permit, verbal) or implied consent. Examples of people who may have implied consent are lawyers, agents, translators, or parents under some circumstances. Only information relevant to the nature of the enquiry may be disclosed.

Refusals to Employees Request to their Personal Information

The company may refuse to provide access to personal information if:

- access may pose a serious threat to life, health, or safety or an individual, or to public health or safety;
- access may unreasonably impact on the privacy of others;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings and the information would not be accessible by the process of discover in those proceedings;
- the information would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- providing access is unlawful;
- denying access is required/authorised by Australian law or Court/Tribunal order;
- there is reason to suspect unlawful activity or serious misconduct is occurring and access is likely to prejudice appropriate action;
- access will prejudice enforcement related activity, or
- access may impact on a commercially sensitive decision-making process.

If a decision is made not to provide access, to provide the information in a different way than requested, or not to correct information, the individual will be advised in writing of the reason, any complaint mechanisms available, and any other prescribed matters. They will also be advised of any steps that could be taken that mean the request would not be refused e.g. narrowing the scope of the request.

Correcting Personal Information

The company has a responsibility to ensure recorded personal information is accurate, up-to-date, complete, not misleading and relevant to the purpose for which it was collected. If an employee believes it is not, they may request that it be corrected, deleted or added to.

Any such formal requests should be referred to the Human Resources function. Information will be updated within 14 days of receipt or request.

Complaints of Breaches

Employees who believe there has been an interference with their privacy may raise a concern internally to the Head of HR either by email or in writing.

The company is required to comply with the Privacy Act 1988 and must comply with Data Breach notification laws. An eligible data breach is one that involves unauthorised access or disclosure or loss of personal information that is likely to result in serious harm to the affected individuals.

Serious harm is not defined and the Company will determine whether a reasonable person would consider the harm to be serious. An example might be an employee's device (phone, laptop, USB, etc) that contains personal information of a client, a supplier, or sensitive company information like commercial details. Another example might be the accidental emailing of personal information to the wrong addressee.

The Act requires that all eligible data breaches be notified to the affected individuals and to the Office of the Australian Information Commissioner (OAIC). Breaches must be notified as soon as practicable. If an employee is not aware whether a breach is eligible, the Company has 30 days to investigate and come to a conclusion. If an employee believes that they may have identified a data breach it is imperative that they immediately contact the IT team (if the data breach occurred through loss of a device) so that the breach can be contained. The second step would be for an employee to directly communicate with their Manager, Compliance Manager or another senior manager.

Policy Breach

If an Employee is found to have breached this policy, the company will take appropriate disciplinary action. Serious breaches of this policy may lead to termination of employment.

Responsibilities

Employees and Contractors are responsible for:

- Adhering to the requirements of this policy or related policies
- Submitting a request in writing if access to records are being sought
- authorising or consenting to an organisation or another person having access to their personal information, if required
- advising HR of any suspected data breach

HR and/or Payroll are responsible for:

- Ensuring only necessary information is collected and that candidates and or employees are aware of why it is being collected.
- Ensuring appropriate storage, security and destruction of all personal information
- Reviewing and responding to requests or complaints under this Policy.
- Ensure only appropriate levels of access to the Flare HR system given to candidates, employees according to the requirements of their role.
- de-identifying information about another person when information is provided

advising impacted individual(s) if a data breach our suspected data breach has occurred

Managers are responsible for:

- Ensuring privacy standards pertaining to this policy are carried out
- Responding and escalating any requests for information or complaints relating to this policy to the Head of HR

Policy owner and Effective Date

The policy owner is the Head of HR, AUB
The effective date of this policy is December 2021
The policy is scheduled for review on December 2022