Privacy

Policy Details

Policy Category:	Organisational Administration	Policy No:	AD010
Created by:	Human Resources	Creation Date:	February 2014
Approved by:	Policy Committee	Last Modified:	November 2018
Status:	Active	Next Review Date:	November 2021

Purpose

The purpose of this policy is to describe how Rise manages the information about individuals the organisation collects in the course of providing its services. This policy is available for viewing on line and can be obtained by interested parties in accessible form free of charge.

Definitions

Staff Denotes employee's trainees and volunteers.

Policy

The framework of the Rise Privacy Policy is determined by the Australian Privacy Principles (APP) as contained in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). The principles are as follows:

APP 1 – open and transparent management of personal information

In order to effectively provide its services, Rise may need to collect from its clients, staff and other stakeholders some or all of the following information:

The types of personal information we collect may include name, date of birth, gender, contact information, credit/debit card information, health information and other information connected with a person's history or relationship to Rise, and the services we provide.

We collect personal information from people who are connected to our operations and activities – including staff, people we support, suppliers, service providers and donors.

We may collect personal information for a number of purposes, including:

- Support services: to provide information about support services, and to evaluate and report on these services
- Volunteering and other support: to assist us with volunteering and other activities where we seek the community's assistance
- Other issues: communicating in relation to our operations, activities and objectives, to verify identity, to improve and evaluate our programs and services and to comply with relevant laws.

- Marketing: to communicate about products, services, donations and events

Where we collect personal information for a specific purpose not outlined above, we will provide a collection notice which explains the primary purpose and any related secondary purposes for which we are collecting personal information.

An individual may access the information about them held by Rise by contacting the relevant Leadership Group member of the service area concerned. An individual, or other external stakeholder, who considers that Rise has breached one of the privacy principles may lodge a complaint in the manner described in the Rise External Complaints and Grievances Policy. An employee or volunteer who considers that Rise has breached their privacy should pursue their complaint using the Rise Volunteer and Employee Grievances and Dispute Resolution policy and procedures.

Rise limits access to information collected about individuals to those staff who have a legitimate need for the information in order to fulfil their duties. All Rise employees and volunteers are required to sign a confidentiality agreement at the commencement of their employment with Rise and again upon cessation of their engagement with the organisation.

APP 2 – anonymity and pseudonymity

APP 2 sets out a requirement that an organisation provide individuals with the option of dealing with it using a pseudonym. This obligation is in addition to the existing requirement that organisations provide individuals with the option of dealing with them anonymously.

Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves.

Where it is reasonable and practicable to do so, Rise will engage with supported individuals who want to remain anonymous or to be identified using a pseudonym.

APP 3 – collection of solicited personal information

An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities, and the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

APP 3 clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent if the collection is also reasonably necessary for one or more of the organisation's functions or activities.

An organisation must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

"Sensitive" information is a sub-set of personal information and is afforded a higher level of protection. It may include:

- 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 preferences or practices; or
- criminal record.

Rise will only seek to obtain personal information that is reasonably necessary for the organisation to provide services to the individual concerned. Rise will only collect personal information from, and with the consent of the individual, or, where the individual is unable to provide information and consent, from, and with the consent of a person or entity acting lawfully on behalf of the individual.

APP 4 – dealing with unsolicited personal information

APP 4 creates obligations in relation to the receipt of personal information which is not solicited.

Where an organisation receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information.

If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the organisation must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

In the event of Rise being in receipt of unsolicited personal information, and provided that information is not of a kind that Rise would reasonably be permitted to collect, Rise will destroy or de-identify that information as soon as practicable, provided it is lawful and reasonable to do so.

APP 5 – notification of the collection of personal information

APP 5 specifies certain matters about which an organisation must generally make an individual aware, at the time, or as soon as practicable after, the organisation collects their personal information.

APP 5 requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information.

Rise will notify individuals of the purpose of the collection of their information and of any organisations to which this information may be disclosed. Rise will also notify individuals about whom it holds information of the way in which they can access and/or correct their information and of Rise's complaints process.

APP 6 – use and disclosure of personal information

APP 6 outlines the circumstances in which an organisation may use or disclose the personal information that it holds about an individual.

APP 6 introduces a limited number of new exceptions to the general requirement that an organisation only uses or discloses personal information for the purpose for which the information was collected. These exceptions include where the use or disclosure is reasonably necessary:

Rise will only use or disclose personal information for the purpose for which the information was collected. Exceptions to this principle will be only those identified in the legislation and include:

- to assist in locating a missing person
- to establish, exercise or defend a legal or equitable claim
- for the purposes of a confidential alternative dispute resolution
- as required or authorised by or under an Australian law or court/tribunal order
- if necessary to lessen or prevent a serious threat to any individual's life, health or safety or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual whose personal information is to be used or disclosed
- if necessary in order for the organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to Rise's functions or activities

The Privacy Act and children's privacy

- The *Privacy Act 1988* (Cth) does not specify an age after which individuals can make their own privacy decisions.
- For consent to be valid, an individual must have capacity to consent. Where consent is required for an organisation or agency to handle the personal information of an individual under the age of 18, the organisation or agency will need to determine on a case-by-case basis whether that individual has the capacity to consent.
- The Office of the Australian Information Commissioner's *Australian Privacy Principle guidelines* state:
- *'As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.*
- *If it is not practicable or reasonable for an organisation or agency to assess the capacity of individuals under the age of 18 on a case-by-case basis, they may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.'*

APP 7 – direct marketing

The use and disclosure of personal information for direct marketing is now addressed in a discrete privacy principle.

Generally, organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met.

APP 7.5 permits contracted service providers for Commonwealth contracts to use or disclose personal information for the purpose of direct marketing if certain conditions are met.

Under APP 7.3, where an individual would not reasonably expect his or her personal information to be used for direct marketing, or the information has been collected from a third party, an organisation may only use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

- the individual has consented to the use or disclosure for this purpose, or it is impracticable to seek this consent
- the organisation has provided a simple means by which the individual can opt out of direct marketing and the individual has not opted out, and
- in each direct marketing communication, the organisation must include a prominent statement telling the individual that he or she may request to no longer receive direct marketing, and no request is made.

APP 7.4 requires an organisation to obtain the consent of the individual before using or disclosing sensitive information for the purpose of direct marketing. Rise will not use or disclose personal information for direct marketing purposes except in the following circumstances: where the individual concerned would reasonably expect that their personal information would be used or disclosed for direct marketing and has not made a request to not receive direct marketing. All direct marketing from Rise will include a prominent statement advising the individual that they may request to no longer receive direct marketing and the manner in which to do this. Individuals may also request Rise not to disclose their personal information to other organisations for the purposes of direct marketing and to provide its source of the individual's personal information.

APP 8 – cross-border disclosures

Before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the organisation. There are a number of exceptions to these requirements.

In the event that Rise has a need to disclose personal information to an overseas recipient, Rise will take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to that information.

APP 9 – adoption, use or disclosure of government related identifiers

APP 9 prohibits an organisation from adopting, using or disclosing a government related identifier unless an exception applies.

Rise will not adopt, use or disclose a government related identifier unless an exception applies as described in the legislation, including for example:

- the use or disclosure is necessary for the organisation to fulfil its obligations to the agency or
- the organisation has been prescribed by regulations to use or disclose a prescribed identifier in prescribed circumstances.

APP 10 – quality of personal information

Under APP 10, an organisation must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete.

For uses and disclosures, the personal information must be relevant, as well as, accurate, up-to-date and complete, having regard to the purpose of the use or disclosure.

Rise will take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. In relation to the use and disclosure of personal information, Rise will ensure that the personal information is relevant, as well as, accurate, up-to-date and complete, having regard to the purpose of the use or disclosure.

APP 11 – security of personal information

APP 11 requires an organisation to take reasonable steps to protect the personal information it holds from interference, in addition to misuse and loss, and unauthorised access, modification and disclosure.

APP 11 requires an organisation to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any authorised purpose. Under APP 11 there are two exceptions to this requirement:

- the personal information is contained in a Commonwealth record, or
- the organisation is required by or under an Australian law or a court/tribunal order to retain the information.

Rise will take reasonable steps to protect the personal information it holds from interference, misuse and loss, and unauthorised access, modification and disclosure. Rise will take reasonable steps to destroy or de-identify personal information it no longer requires for an authorised purpose unless:

- the personal information is contained in a Commonwealth record, or
- the organisation is required by or under an Australian law or a court/tribunal order to retain the information.

APP 12 – access to personal information

The APPs separate the access and correction requirements into two separate principles.

APP 12 requires an organisation to give an individual access to the personal information that it holds about that individual, unless an exception applies. Examples of exceptions can be found at the Office of the Australian Information Commissioner website: oaic.gov.au

There is a requirement for organisations to respond to requests for access within a reasonable period. In addition, organisations must give access in the manner requested by the individual if it is reasonable to do so. If an organisation decides not to give an individual access, it must generally provide written reasons for the refusal and the mechanisms available to complain about the refusal.

If an organisation charges an individual for giving access to the individual's personal information, the charge must not be excessive, and must not apply to the making of the request.

Rise will provide to an individual access to the personal information it holds about the individual within a reasonable period, and in the manner requested by the individual if it is reasonable to do so, and provided an acceptable exception does not apply. Generally, Rise will not charge individuals for access to the information unless there is sound justification for doing so, in which case the charge will be as minimal as possible.

Rise will not give an individual access to their personal information if:

- Rise has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to Rise's functions or activities has been, is being or may be engaged in, and

- giving access would be likely to prejudice the taking of appropriate action in relation to the matter.

In the event that Rise declines to give an individual access to their information, Rise will provide written reasons for the refusal and advice on the mechanisms available to complain about the refusal.

Requests from employees for access to their employee records will be considered on the merits of the case. Rise may refuse to make available to an employee some records pertaining to their employment. The Privacy Act exempts employee records from the Act in respect of current or former employee records.

APP 13 – correction of personal information

APP 13 introduces some new obligations in relation to correcting personal information. The APPs remove the former National Privacy Principle requirement for an individual to establish that their personal information is inaccurate, incomplete or is not up-to-date and should be corrected.

APP 13 now requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:

- the organisation is satisfied that it needs to be corrected, or
- an individual request that their personal information be corrected.

Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

APP 13 contains provisions in relation to associating a statement with the personal information if the organisation refuses to correct the information and the individual requests a statement to be associated.

An organisation must also respond to a correction request or a request to associate a statement by the individual within a reasonable period after the request is made and must not charge the individual for making the request, for correcting the personal information, or for associating the statement with the personal information.

When refusing an individual's correction request, an organisation must generally provide the individual with written reasons for the refusal and notify them of available complaint mechanisms.

Rise will take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:

- the organisation is satisfied that it needs to be corrected, or
- an individual request that their personal information be corrected.

In the event that Rise refuses an individual's correction request, Rise will provide the individual with written reasons for the refusal and notify them of available complaint mechanisms.

Breaching this policy may lead to the application of the Performance Management Policy.

Procedure

N/A

Cross reference to relevant policy

Intellectual Property

Communications

Forms pertaining to this policy are/location

Confidentiality and Intellectual Property Agreement