Privacy Policy

Contents

Policy Owner and Approval	▪ The Owner of this policy is the Chief Executive. ▪ This Policy has been approved by the Board. ▪ The Committee responsible is the Governance Committee.
Review Date	February 2019
Effective Date	14 May 2012
Breaches of Policy	Breaches of this Policy may be considered a disciplinary matter by Southern Response.

Introduction

Purpose and Scope	The purpose of this Privacy Policy is to provide 'best practice' guidelines to ensure compliance by Southern Response Personnel with the provisions of the Privacy Act 1993 (the Privacy Act). This policy is designed to apply the concepts contained in the Information Privacy Principles ('IPPs') to the Southern Response environment and was developed with reference to the Southern Response Privacy Framework and Strategy. This Policy applies to any Southern Response Personnel who deal with Personal Information relating to customers, Personnel and/or members of the public. This Policy also applies to any Southern Response contractor who may be required to deal with Personal Information. This policy accords with the values and other core principles of Southern Response (the spirit of the policy).
Definitions	Definitions relating to this Policy can be found as Appendix 1.

Policy

Collection of Personal Information

Under Information Privacy Principle 1 of the Privacy Act ('Purpose of collection of personal information', Personal Information cannot be collected by an agency unless:

- the information is collected for a lawful purpose connected with a function or activity of the agency; and
- the collection of the information is necessary for that purpose.

The purposes for which Personal Information is collected and used by Southern Response include:

- evaluating, processing, managing and settling any claims, and undertaking other functions that are necessary for, or incidental to, evaluating, processing, managing and settling such claims;
- strategic budgeting and forecasting;
- administering and planning human resources (including health and safety);
- audit;
- reporting information to Government bodies or other agencies to meet legislative or governance obligations; and
- providing information to AMI Insurance in the administration of customers' insurance policies.

Southern Response Personnel that have access to Personal Information in order to do their jobs include:

- Southern Response claims Personnel responsible for claims management and settlement; and
- Human Resources Personnel responsible for any matters that may arise for a Southern Response employee.

Under IPP 3 ('collection of information from subject'), when collecting personal information from an individual, Southern Response will use reasonable endeavours to bring the following to the individual's attention:

- the purposes for which the personal information is collected;
- identification of the personnel positions which will have access to the personal information;
- details of Southern Response (as holding entity) and its Privacy Officer;
- questions required to be answered by law and which law this is required under (e.g. statistical information under the Statistics Act 1975);
- compulsory/optional questions and the consequence (if any) of not providing the requested information; and
- that the individual has a right to access and correct his or her personal information.

When collecting Personal Information and before it is used, it is important that the Personal Information is accurate, relevant, up to date and not misleading.

Informed Consent

If Personal Information is used for the purposes stated for its collection and use (see Collection of Personal Information above) then further consent or authorisation is not required.

If a matter arises not contemplated by the purposes stated for the Collection of Personal Information then consent is required.

This should be informed consent and the person that has had their Personal Information collected must be aware of the intended use. It must be made clear that there is no pressure to give consent and if consent is given it should be carefully recorded.

Types of Personal Information - Customers

For the purposes identified here or in Collection of Information above, Personal Information collected and maintained by Southern Response typically comprises the following:

- name;
- contact details;
- bank information;
- insurance policy cover/information;
- claim history/information;
- correspondence between Southern Response, AMI Insurance and the customer; and
- personal information relating to the claim settlement process, including information about the customer's house and land.

Types of Personal Information – Southern Response Staff

For the purposes identified here or in Collection of Personal Information above, Personal Information collected and maintained by Southern Response typically comprises the following:

- name;
- contact details;
- date of birth;
- gender;*
- emergency contacts;
- nationality/citizenship;
- ethnicity;*
- department/unit and location;
- URL (internet addresses) of pages and sites accessed by individuals using Southern Response Internet links;
- computer user names and passwords;
- other Personal Information collected during the recruitment process including qualifications, previous work experience, evaluative material including interview notes and reference checks and results of other screening procedures e.g. criminal record checks; drivers licence histories; criminal convictions etc;
- salaries;
- details of employment agreements;
- bank and tax information;
- languages spoken;
- photographs (for identification purposes);
- evaluative and non-evaluative information relating to performance reviews;
- correspondence between Southern Response and the member of Personnel; and
- Personal Information relating to any investigation and resolution of a disciplinary matter.

*this usually represents statistical information required for monitoring equal employment opportunities within Southern Response. This information is not collected for the purposes of discrimination on any prohibited grounds contained in the Human Rights Act 1993.

Exceptions to IPP3

Southern Response takes all reasonable steps to ensure an individual is aware Personal Information is being collected about them and the purpose of such collection, unless the situation is covered by one of the applicable exceptions set out in IPP3 of the Privacy Act:

- the individual concerned authorises non-compliance;
- non-compliance does not prejudice the interests of the individual concerned;
- non-compliance is necessary to avoid prejudice to the maintenance of law;
- compliance would prejudice the purposes of collection;
- compliance is not reasonably practicable in the circumstances of the particular case; or
- the information will be used in a form in which the individual is not identified.

Collection of Personal Information from Third Parties

Southern Response usually collects information directly from the individual concerned.

It may collect personal information from a third party if the situation is covered by IPP2 of the Privacy Act, which includes where:

- the information is publicly available information;
- the individual concerned authorises collection of the information from someone else;
- non-compliance would not prejudice the interests of the individual concerned;
- non-compliance is necessary to avoid prejudice to the maintenance of the law;
- compliance would prejudice the purposes of collection;
- compliance is not reasonably practicable in the circumstances of the particular case; or
- the information will not be used in a form in which the individual concerned is identified.

Disclosure of Personal Information to Third Parties

Southern Response is subject to the Official Information Act 1982 ('OIA'). If there has been a request by a third party for Personal Information then this request will be treated in accordance with the OIA.

Southern Response may disclose Personal Information to third parties where:

- there has been a request under the OIA for the release of Personal Information, and:
  - there are no conclusive reasons for withholding the information (section 6 OIA);
  - there are no special reasons (section 7 OIA); or
  - there are no other reasons (section 9 OIA) including no privacy interest to protect, and/or there is a strong public interest reason for the release of the information;
- there is another legal requirement to release the information (e.g. statutory, contractual); or
- there is an emergency situation under which a member of Personnel's emergency contact details are released to a member of Southern Response's Management or an appropriate third party agency (e.g. Police).

Southern Response may disclose personal information to third parties in the following circumstances:

- it is for one of the purposes stated in Exceptions to IPP 3 above; and/or
- the situation is covered by one of the exceptions set out in IPP 11 (Limits on disclosure of Personal Information), including when:
  - the information is publicly available information;
  - disclosure is to the individual concerned or is authorised by the individual concerned;
  - non-compliance is necessary to avoid prejudice to the maintenance of the law;

- non-compliance is necessary to prevent or lessen a serious and imminent threat to public or individual health and/or safety (note that disclosure should be to someone who can do something about it e.g. the Police); or
- the information is in a form by which the individual concerned cannot be identified.

Release of Personal Information by Telephone

Southern Response Personnel do not give Personal Information out over the phone or send Personal Information electronically unless the member of Personnel is reasonably satisfied that the receiver is:

- a person to whom Personal Information may be disclosed; or
- the individual to whom the Personal Information relates.

Steps Personnel should take to ensure identification of the receiver include:

- calling the individual back at a known telephone number;
- verifying address and full names;
- asking for the customer's policy and/or claim number; or
- recognition of the receiver's voice.

Outcome of Disciplinary Procedures

If Southern Response receives a complaint about a member of Personnel, thereby invoking any disciplinary procedure, the complainant is to be told from the outset that while they will be advised that an outcome has been reached, they will not receive full details of the action (if any) taken against the member of Personnel.

Enquiries from Police or other Government Officials

If a Southern Response member of Personnel receives a request from the Police, a process server from the Court or other government official (including immigration) to access Personal Information , the request should be escalated to Southern Response's Privacy Officer (where the information requested concerns a customer) or Human Resources Advisor (where the information requested concerns a staff member).

Whilst Personal Information may be released to these agencies to avoid prejudice to the maintenance of the law (including the prevention, detection, investigation, prosecution and punishment of an offence) it is not Southern Response's policy to provide open access to such information. There will be times when it is appropriate for these agencies to obtain a warrant from the Court, ordering the release of the information.

If the Police are seeking the assistance of a member of Southern Response Personnel to contact a team member:

- in the case of accident, sudden death or emergency, then reasonable assistance will be given to find the person concerned and to ensure that person has the opportunity to speak to the Police in private; or
- in non-emergency cases (e.g. return of a stolen wallet), the Southern Response member of Personnel will make a reasonable effort to contact the person concerned and advise them to contact the Police.

Access to and Correction of Personal Information

Any person may ask Southern Response whether Personal Information is held about him or her and have access to such information if it exists subject to the exceptions contained in Part 4 of the Privacy Act described below. Access is not limited to 'the customer file' and may include any notes, information and/or material in separate files.

The right extends to an agent appointed by the individual. Such an appointment must be in writing or, in urgent situations, Southern Response can confirm orally with the individual that the person is authorised to access the information.

Southern Response communicates decisions on requests as soon as practicable but not later than 20 working days, pursuant to the statutory timeframes within the Privacy Act.

If the individual has requested urgency then they are required to give reasons.

Requesters can seek the correction of Personal Information held by South Response. If the requester seeks to correct information and this correction is not accepted by Southern Response, then the requester is given the opportunity to have a statement of correction held with the information. The information and correction is held in such a way that anyone accessing the file or record will understand the two positions that are held on file.

If a Southern Response member of Personnel is aware that incorrect information is held, they should take all practicable steps to have the file corrected immediately. Any change should be noted carefully to ensure that an adequate audit trail of changes exists.

Declining Requests: Part 4 of the Privacy Act

A request for some or all information held by Southern Response may be declined for the reasons set out in Part 4 of the Privacy Act, which include:

- endangerment of the safety of any individual;
- maintenance and enforcement of the law;
- protection of trade secrets;
- release will result in the unwarranted disclosure of the affairs of another individual;
- disclosure is of evaluative material thereby breaching an express or implied promise to keep it confidential;
- disclosure is likely to prejudice the physical or mental health of the individual;
- disclosure would breach legal professional privilege; or
- the request is frivolous or vexatious or the information is trivial.

If the request for the information is declined, Southern Response will explain why the request was declined and advise the requester of their right to complain to the Office of the Privacy Commissioner.

Storage and Security of Personal Information

Southern Response shall ensure that information (both paper and digital) is protected by such security safeguards as are reasonable in the circumstances to protect Personal Information from loss, unauthorised access, use, modification, disclosure and other misuse.

Personal Information Stored Digitally

Personal information stored digitally:

- is restricted to staff who are authorised for the purpose outlined in Collection of Personal Information above, using network and/or other security setting and access/use rights systems. This may include “write” access to those authorised to add to or change an electronic file; and
- is deleted from the system when no longer required.

Personal Information Stored Physically

Personal information stored physically:

- is protected by such security safeguards as it is reasonable in the circumstances to take, including:
  - ensuring Personal Information is not exposed to unauthorised people;
  - restricting unsupervised building access to Southern Response and Arrow employees only; and
- is only accessible from storage when the person accessing the Personal Information logs their details in a register recording access and return.

For records maintained in long-term storage by Southern Response's contracted provider of secure storage, access logs will be maintained in electronic format. This log will record the Personnel member's name, business unit/pod, date of request and the date of return.

Sensitive Personal Information

Southern Response recognises that some Personal Information can be more sensitive than other Personal Information. To determine sensitivity, the question is whether the person in question will suffer any actual loss or humiliation, loss of dignity and injury to feelings if the information is lost or inappropriately accessed or used; for example inappropriate disclosure of an individual's health.

Sensitive Personal Information recorded digitally:

- is restricted to staff who are authorised for the purpose outlined in Collection of Personal Information above, using network or other security setting and access/use rights systems; and
- is deleted from the system when no longer required

Sensitive personal information recorded physically:

- must be kept secure;
- if distributed through internal mail, must be sent in a sealed envelope (rather than the reusable internal mail envelopes), marked "Private and Confidential" and if deemed necessary the words "To be Opened by the Addressee Only" should be added; and
- must be separate from any regular personal file/record and accessible only to the parties directly involved.

If sent by facsimile then the receiver should be telephoned prior to sending the fax to ensure they are waiting to receive it.

Email

Email is not a guaranteed secure or private form of communication.

It is important to note that an email sent or received by Southern Response Personnel may be subject to requests under the Official Information Act and/or Privacy Act.

Employees' Personnel Files

Personal Information gathered from and/or about a successful applicant for employment at Southern Response will be retained on their personnel file for the purposes of considering and evaluating any other application they may make for employment or appointment by Southern Response in any role other than that which they originally applied to Southern Response.

Unsuccessful Applications

Details of applicants not short listed for interview are to be confidentially destroyed following the closing of the vacancy.

Evaluative Information on Employees

Evaluative information is placed in a sealed envelope and sectioned off from non-evaluative information in the personnel file. This information is available to Personnel who are normally party to the evaluation process or who require it for a further authorised and specific purpose. It is not automatically available to the member of Personnel concerned and should be removed prior to an individual viewing their personal file/record.

Non - Evaluative Information on Employees

Non-evaluative information (for example appointment letters, employment agreements, salary histories, leave records etc.) are included in personal files and sectioned off from evaluative material as described above. The information is made available to any member of Personnel who has a purpose for reviewing this information. The member of Personnel concerned also has access to this information.

All personal records are retained only for as long as needed, and then disposed as either archives or destroyed based on their values.

Work Taken Out of a Unit

It is recognised that there are critical times when Personnel will need to remove Personal Information from a Southern Response business unit (e.g. a meeting at EQC or Ministry of Business, Innovation and Employment Mediation Services). If it is necessary for the purposes identified in Collection of Personal Information above, that Personal Information is to leave Southern Response premises, Personnel must take the following precautions:

- Personal Information travels securely – in a briefcase or suitable container, fully enclosed envelope, file or folder;
- multiple instances of electronic Personal Information are not copied to removable storage media or removed from secure systems.
  Examples of this type of information include:
  - databases of customer information;
  - databases of Personnel information; and
  - spreadsheets of personal information;
- if travelling by motor vehicle:
  - it is preferable that such information is not left unattended in or near the motor vehicle; and
  - the briefcase, envelope, file or folder containing the Personal Information is not visible/easily accessible; and
- during the time the Personal Information is away from Southern Response, all reasonable steps are taken to ensure that it is not accessed by unauthorised people.

Sharing of Personal Information between Employees

Personal Information is accessed by Personnel who need the information to do their job. Accordingly Personal Information is not shared within Southern Response unless it is for a legitimate purpose of Southern Response.

Personnel seeking assistance or guidance in the management of an issue from colleagues/peers do not usually identify the person concerned. The person may be identified if necessary.

No Personal Information relating to medical conditions/disabilities is shared without the informed consent of the individual unless it is necessary to prevent or lessen a serious and imminent threat to individual or public safety, and it is provided to a responsible Manager only.

Retention and Disposal of Personal Information

Personal Information is not to be kept for longer than is required for its proper purpose without consent from the individual concerned (unless required by statute or other regulation). The test is whether the retention of Personal Information is necessary for the legitimate purposes contemplated and notified at the time of collection.

Personal Information must be destroyed with safeguards taken to prevent inadvertent disclosure (e.g. shredding or locked confidential destruction bins).

Misuse of Personal Information

Without limiting the definition of misuse of Personal Information, the following practices are unacceptable to Southern Response:

- intentionally breaching the Privacy Act and the Official Information Act;
- reading or copying Personal Information to which the reader/copier has no authorised access;
- divulging Personal Information given under an express undertaking it will remain confidential or intentionally divulging Personal Information to any person who is not an authorised recipient of that information without lawful excuse;
- intentionally introducing false or misleading material into any Southern Response database or file/record, or falsifying such records or deleting such records without authorisation;
- using Personal Information for any purpose other than the purposes identified in Collection of Personal Information above, unless the individual consents; and
- inappropriate browsing or copying of Personal Information to which the reader/copier has no legitimate business reason for accessing. For example, this may include information relating to family members, friends or persons in the media.

Use of Identifiers

It is acknowledged that Southern Response uses numbers for identification and operational efficiency and it is recognised that Personnel and customers' names are important. Unless required by law, Southern Response does not use the same number as another agency to identify a member of Personnel.

Responsibility for Compliance

All Southern Response Personnel are responsible for compliance with this Policy.

To assist with compliance:

- Southern Response has appointed a Privacy Officer;
- all managers of Personnel encourage compliance with this Policy and put in place processes to facilitate compliance;
- it is the responsibility of each customer and member of Personnel to contact the relevant unit within Southern Response if they require changes to Personal Information that has been provided;
- to assist managers of Personnel, Southern Response provides training on Privacy matters at personnel induction and meets with teams regularly to discuss Privacy matters relevant to their day-to-day operations;
- the Privacy Officer updates the "All About Privacy" page on the Southern Response Intranet (Southsite) as required to assist Personnel maintain currency with this Policy and share ideas and issues. Other meetings for the same purposes are arranged as needed; and
- all staff are required to notify their Team Manager or the Privacy Officer immediately should they become aware of any breach, or potential breach, of the Privacy Act or this Policy. If the Privacy Officer is not available, the Legal Risk Manager is to be notified.

The Privacy Officer

The Privacy Officer is a role required by the Privacy Act.

Relevant Links

Procedures

- Handling Privacy and Official Information Act Requests Procedure.
- Privacy Breach Investigation Process

Standards

- Southern Response's IT Standards
- Acceptable Use
- Network Security
- Internet Security
- Email Security
- User Administration
- Work Station
- Wireless
- Virus Protection

Relevant References and Resources

- Privacy Act 1993
- Official Information Act 1982
- 15. Use of Information Resources and Security Policy
- 16. Official Information Policy
- 18. Ethical Behaviour Policy
- 19. Solving Employment Problems Policy
- Privacy Framework and Strategy
- Office of the Ombudsman
- Office of the Privacy Commissioner

Appendix 1 – Definitions

Evaluative Material

Some Personal Information is created and recorded about individuals in an evaluative context. This material is defined in section 29 of the Privacy Act, and includes evaluative or opinion material compiled solely for the purpose of determining:

- the suitability, eligibility, or qualifications of the individual to whom the material relates:
    - for employment or for appointment to office;
    - for promotion in employment or office or for continuance in employment or office;
    - for removal from employment or office;
    - for the awarding of contracts, awards or other benefits; or
- whether any contract, award or benefits should be continued, modified or cancelled.

Examples include employment interview notes, test results, references, employment consultant reports and employment promotion evaluation notes.

Personal Information

Personal information means information about an identifiable individual.

Information as defined in the dictionary is that which informs, instructs, tells or makes aware. Personal information can be anything which instructs, tells or makes (another) aware about an identifiable individual.

Sensitive Personal Information

A subset of Personal Information. Sensitive Personal Information is typically determined by considering the potential or actual loss of dignity, humiliation or injury to feelings or unfairness that would result if that information is lost, inappropriately accessed or used.

Unit

Within this policy the use of the word “unit” refers to any team, service unit or department of Southern Response as appropriate in the particular context.

Personnel

Applies to all employees and other personnel providing services to Southern Response (e.g. independent contractors), together defined as “Southern Response Personnel”.