

## PRIVACY AND CONFIDENTIALITY

### Purpose

Spinal Life Australia Ltd respects the privacy of all people including members, clients/beneficiaries, employees, volunteers, donors, business partners, contractors and online users, and is committed to safeguarding the personal information provided to us.

The purpose of this privacy and confidentiality policy is to:

- clearly communicate the personal information handling practices
- enhance the transparency of our operations, and
- give individuals a better and more complete understanding of the sort of personal information we hold, and the way we handle that information.

We are committed to supporting the provisions of the Commonwealth Privacy Act 1988 (Privacy Act) and the Australian Privacy Principles (APPs) with respect to the consideration, collection, dealing, integrity, access to and correction of, personal information.

### Scope

This policy applies to all organisation members, volunteers, employees, clients/beneficiaries, donors, business partners, contractors and online users.

The Privacy Act and this Privacy and Confidentiality policy does not apply to acts or practices which directly relate to employee records of current and former employees.

### Objectives

Spinal Life Australia provides a range of services with the intent purpose to re-build lives, promote independence and prevent injuries. A range of high-quality service programs has been designed to empower clients and members either in their homes, at the workplace or in the community.

Personal assistance in the home, employment assistance, advocacy on a wide range of issues, and healthcare and lifestyle advice and support are some of the services provided to eligible people.

In carrying out this mission the organisation engages volunteers and employees, and receives donations, funding and support from members of the community, corporations, groups and governments.

In addition to the services which we provide from funds donated by the public, or fee-for service, the organisation also holds contracts to deliver State and Commonwealth government programs. In providing such services, we comply with the relevant state or national privacy principles and any additional obligations under the contract.

This policy is outlined in three sections:

**Part A** – Personal Information Handling Practices’ explains our general information handling practices across the organisation including information about how we collect, use, disclose and store your personal information.

**PRIVACY AND CONFIDENTIALITY**

**Part B** – Files’ offer further detail by explaining our personal information handling practices in relation to specific organisation functions or activities such as contact lists, public awareness and education files and enquiries. Here you can find out what sort of records we keep and why. You may find this section helpful if, for example, you have made an enquiry and wish to know how we manage our contact lists and enquiries files.

**Part C** – Confidentiality. This section explains practices taken by the organisation to ensure confidentiality of information.

**Part A – Our Personal Information Handling Practices****Our obligations under the Privacy Act**

This Privacy and Confidentiality policy sets out how we comply with our obligations under the Privacy Act. We are bound by the Australian Privacy Principles in the Privacy Act which regulate how organisations may collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.

**Collection of Personal and Sensitive Information**

If you would like to access any of our services or supports on an anonymous basis or using a pseudonym, please tell us. If this is possible and lawful, we will take all reasonable steps to comply with your request. However, we may not be able to provide the services or supports in question if we are not provided with the personal information requested.

We will only collect information which contains government related identifiers where it is reasonably necessary to verify identity for the organisation’s functions and activities, or where required by law. For example, drivers licence numbers, passport numbers, tax file numbers.

The nature and extent of personal and sensitive information collection by us varies depending on your particular interaction with us.

We collect personal and sensitive information from clients/beneficiaries, members, donors, business partners, contractors, our people and online users. Further information about the kind of information collected from each of these groups and the usage of such information is detailed below.

**Our Clients and Beneficiaries**

Kind of information that may be collected if required:

- contact details (name, address, telephone numbers, email etc)
- personal details (date of birth, gender, citizenship, funding details/agencies, income)
- employment status and details (job title, employer name, supervisor and contact details)
- goals, interests, skills, experience
- sensitive information (family background, relationships, issues, culture and communication details, birthplace, language, ATSI status, DS NMDS)
- supports clients may have in the community, emergency contacts, nominated representative or advocate
- where applicable, details of legal guardian, attorney appointed under an enduring power of attorney or advance health directive, a guardian or administrator appointed by law or Court
- health information and/or medical history (injury details, primary disability, other disabilities, cause, medical conditions, date of disability, functioning/limitations, medications, medical certificates, health reports, barriers, support requirements, assessment summaries)

**PRIVACY AND CONFIDENTIALITY**

- credit card numbers or bank account details.

How the information is collected:

- service registration and applications
- service agreements and support plans
- intake processes
- interviews, meeting face to face
- online registrations, or enquiries
- telephone
- referrals for services and programs received internally and from external third parties.

Purpose for which we use the information:

- to plan and provide our services and supports
- to assess and provide clients/beneficiaries with the most appropriate services for their needs
- to enable communication with emergency contacts, advocates, employers (if required), treating professionals, govt. departments
- to provide equipment prescriptions to the client
- to determine eligibility to access service/s based on guidelines
- to develop individual support plan
- to meet any requirements of government funding for programs, and reporting such as NMDS
- to monitor and evaluate existing services and plan for future services and programs
- to apply for equipment funding to funding providers
- to determine appropriate referrals and management to other services
- to determine billing and invoice requirements
- to develop a service and track progress and outcomes of each intervention
- to monitor and measure quality of service provision
- data input for business, operational and resources
- to produce reports and for research purposes which may involve contracted organisations
- to comply with legal requirements.

#### *Direct Debit Agreements*

- how it works - when a person or organisation nominates to pay for services by direct debit they are automatically entering a direct debit agreement. Depending on the terms of the agreements payments are generally processed quarterly and credit card information is securely stored. Credit card details are held by the bank.
- opting out – direct debits will be processed in accordance with the agreement unless changed or cancelled in writing.

#### **Our Donors**

Kind of information that may be collected if required:

- contact details (name, address, telephone numbers, email etc)
- personal details including date of birth, gender, income
- areas of interest
- donation history

**PRIVACY AND CONFIDENTIALITY**

- credit card numbers or bank account details of all our donors
- expiration date of credit card.

How the information is collected:

- communications, email, flyers, registration brochures and booking forms
- online registration
- telephone – call centre.

Purpose for which we use the information:

- to provide our services
  - to process donations and provide accurate receipts
  - to facilitate on-going fundraising and marketing activities
  - to comply with legal obligations
- to provide transparency related to donated funds, particularly for Appeals for public donations.

*Monthly Direct Debit Donation Agreements*

- how it works - when a person or organisation nominates to leave a monthly gift the donor is automatically entering a monthly direct debit donation agreement. Donations are processed mid-month and credit card information is securely stored.
- opting out – donations will be made each month unless changed or cancelled in writing by the donor.

**Our Business Partners and Contractors**

Type of information that may be collected, if required:

- contact person's name, the name of the organisation which employs the person, telephone numbers, fax number, street and postal address and position title
- areas of interest by category and industry
- bank account details (if we are to receive payment or make payment for services or goods received or provided)
- Australian Business Number (ABN)
- type of support or service (eg. workplace giving, goods in kind, equipment, product, service or program support, volunteering)
- transaction history, quotes or pricing
- quality accreditation assurances, insurance status, compliance and contractual, licensing or regulatory records.

How the information is collected:

- communications, email, flyers, registration brochures and booking forms
- contracts, agreements or memorandum of understanding documents
- preferred supplier documentation and register
- online registrations or enquiries
- telephone – call centre
- face to face meetings, interviews.

Purposes for which we use the information:

**PRIVACY AND CONFIDENTIALITY**

- to provide our services
- to process donations and provide accurate receipts
- to pay for services and goods
- to establish and manage partnerships and/or preferred suppliers
- to receive services from you or the organisation which employs you
- to manage our relationship with the business partner
- to provide information about our services
- to update the company on our appeals for public donations, programs and services
- to provide validation for meeting quality assurance, contractual, licensing, professional accreditations or legal obligations.

**Our People (volunteers, employees, delegates) and candidates for volunteer work and prospective employees**

Type of information that may be collected, if required:

- contact details (name, address, telephone numbers, email etc)
- personal details including personal details of emergency contact person(s)
- date of birth
- country of birth, citizenship, residency and/or visa details, right to work in Australia (VEVO check)
- ID (Govt. related identifiers for example Tax File Number, Drivers Licence, Positive Notice Card)
- details of current/previous employment or volunteer involvement
- skills and experience, work history and referees contact details
- languages spoken and written
- qualifications, current professional accreditations/registrations (RN, EN, OT), professional memberships, if required
- information and opinions from referees for prospective employees and candidates for volunteer work
- a Police Check will be required for roles in accordance with the Disability Services Act and Department of Communities Criminal History Screening requirements, and Working with Children (Risk Management and Screening) Act 2000 requirements, or Disability Employment Services contractual and legal requirements. Individuals will be required to provide certain information for a Police Check. There are different arrangements for Police Checks in each state and territory of Australia. In most cases evidence of the Police Check will be received directly by us from the govt agency, or sometimes the candidate will provide this evidence which is securely stored.
- in some situations, it is necessary for us to collect or receive information about an individual's health. In this circumstance, we will advise the individual why the information is being collected and whether and to whom it will be released.
- in some situations, we will collect Pre-Employment Health Checks information, as part of the recruitment process of employees and in accordance with the Worker's Compensation and Rehabilitation Act 2003.

How the information is collected:

- position applications and expressions of interest documentation
- online registration and applications
- resumes, assessment instruments

**PRIVACY AND CONFIDENTIALITY**

- recruitment processes conducted in house
- recruitment agencies
- telephone
- email
- government agencies.

Purpose for which we use the information:

- to provide our services
- to process an application to become a volunteer or employee of our organisation
- to facilitate a placement in an appropriate service or position
- to assist with services whilst an individual is employed or engaged as a volunteer with us
- to provide feedback on performance as a volunteer or employee
- to meet legislative responsibilities to all volunteers and employees
- to obtain feedback from individuals about their experiences
- to assist us to review and improve our programs and services
- to keep individuals informed about our developments and opportunities
- to provide information about our services
- to facilitate further involvements with us (eg. clients, disability supports, membership, networks, donors)

**Our Members**

Type of information which may be collected, if required:

- contact details (name, address, telephone numbers, email etc)
- date of birth, gender
- injury related details and disability type
- date of membership commencement and renewal
- culture and communication details, birthplace, language, ATSI status
- employment status, hobbies, interests, skills
- credit card details
- expiration of credit card details
- type of membership group (Ordinary, Associate, Junior, Complimentary or Life).

How the information is collected:

- membership application and renewal forms
- service or activity, event registration forms
- online registration
- telephone.

Purpose for which we use the information:

- to provide our services
- to determine eligibility of membership type
- to provide communication updates and ensure transparency
- to mail the Advocate and other publications
- relating to donated funds, particularly Appeals for public donations
- our normal business practices
- to process membership fees and provide accurate receipts

**PRIVACY AND CONFIDENTIALITY**

- to facilitate ongoing fundraising and marketing activities
- to provide information about us
- to receive invitations to upcoming events and activities
- to promote involvement with member networks and community development activities
- to recognise your support of us.

**Online Users**

To the extent that this Privacy and Confidentiality policy applies to online privacy issues, it is to be read as forming part of the terms and conditions of use for Spinal Life Australia's website.

The online Privacy Statement informs visitors to the website to be aware that Spinal Life Australia:

- respects the right to privacy of all individuals and organisations
- does not collect any personal information about its donors and web visitors, except that which is knowingly and specifically supplied
- is committed to ensuring the privacy of individuals' personal information
- always provides individuals with the opportunity to receive no mailings or contacts from us
- complies with the Privacy Act; and
- complies with the [Australian Direct Marketing Association's \(ADMA\) Code of Practice](#)

Type of information which may be collected, if required:

- contact details (name, address, telephone numbers, email etc)
- organisation details
- credit card number and details
- expiry date of credit card
- service feedback and enquiries
- personal information
- donation information
- classifieds, advertising copy and details
- non-personal information eg, visitor navigation and statistics
- subscription requests
- server address, browser type, date and time of visit

Purpose for which we use the information:

- to process donations, merchandise orders, online bookings, loans, purchases/transactions, subscriptions (e.g. booking education workshops, programs, events, specific activities, resources and equipment)
- to receive feedback and enquiries and distribute the information to appropriate departments and services
- to provide correspondence
- to keep donors and web visitors up to date about changes to the website or activities
- to undertake surveys
- to facilitate classifieds communication for the advertising service
- to analyse website usage and make improvements to the website, non-personal information and web usage data such as numbers and frequency of visitors, pages accessed and files downloaded. This helps to determine how much web visitors use parts of the site, how many people visit on a regular basis and the usefulness of the webpages. This information doesn't tell us anything about who individuals are or where they live – it simply allows for monitoring of the effectiveness of the website.
- We do not match the personal information collected with the non-personal information.

## PRIVACY AND CONFIDENTIALITY

### *Additional information*

The website may from time to time contain links to other websites. We in particular stress that when an online user accesses a website that is not the Spinal Life Australia website, it may have a different Privacy policy. To verify how that website collects and uses information, the user should check that particular website's policy.

### *Users of the Classifieds section on the website*

People submitting and advertising products or services in the website's Classified section are advised that information provided may be viewed and used by other users of the website's Classified section through the internet. Therefore, information posted there is 'disclosed' to the open and international internet user community.

### **How We Collect Information**

Where possible, we collect your personal and sensitive information directly from you. We collect information through various means, including telephone and in-person interviews, appointments, forms and questionnaires. If you feel that the information that we are requesting, either on our forms or in our discussions with you, is not information that you wish to provide, please feel free to raise this with us.

In some situations, we may also obtain personal information about you from a third party source. If we collect information about you in this way, we will take reasonable steps to contact you and ensure you are aware of the purposes for which we are collecting your personal information and the organisations to which we may disclose your information, subject to any exceptions under the Act.

In a situation where unsolicited personal information is received, and if lawful and not in a Commonwealth record, the information will be returned to the sender, destroyed or de-identified as soon as practicable.

### **Health Information**

As part of administering our services, we may collect health information. For example, we collect health information (such as medical history) from some clients/beneficiaries and members participating in our programs. When collecting health information from you, we will obtain your consent to such collection and explain how the information will be used and disclosed.

If health information is collected from a third party (such as your doctor), we will obtain your consent to collect this information and will explain to you how this information will be used and disclosed.

We will not use health information beyond the consent provided by you, unless your further consent is obtained or in accordance with one of the exceptions under the Privacy Act or in compliance with another law. If we use your health information for research or statistical purposes, it will be de-identified.

### **Use and Disclosure of Personal Information**

We only use personal information for the purposes for which it was given to us, or for purposes which are related to one of our functions or activities. We does not sell or rent information about stakeholders.



**PRIVACY AND CONFIDENTIALITY**

We may share your personal information with our associated operational divisions, such as relevant Member and Client Services programs, Personal Support and Home Care Services programs, Community Development programs such as Member Networks, Fundraising, Communications and Injury Prevention programs, and support services under normal business practice in Finance and Quality administration, Human Resource Management, including the internal Workplace Health and Safety office where relevant, for recruitment, learning and development, and administration, and technology support services.

For the purposes referred to in this Privacy and Confidentiality policy (discussed above under '*Collection of Personal and Sensitive Information*'), we may also disclose your personal information to other external organisations, in accordance with the Privacy Act and obtain your consent where required, including:

- Government departments/agencies who provide funding for our programs and services
- Contractors who manage some of the services we offer to you, such as distribution centres who may send information to you on behalf of us. Steps are taken to ensure they comply with the APPs when they handle personal information and are authorised only to use personal information in order to provide the service or to perform the functions required by us
- Doctors and health care professionals, who assist us to deliver our services
- Other regulatory bodies, such as WorkSafe (WHSQ)
- Referees and former employers of our employees and volunteers, and candidates for employee and volunteer positions; and
- Our professional advisors, including accountants, auditors and lawyers.

Except as set out above, we will not disclose an individual's personal information to any other third party unless one of the following applies:

- the individual has consented
- the individual would reasonably expect us to use or give that information for another purpose related to the purpose for which it was collected (or in the case of sensitive information – directly related to the purpose for which it was collected)
- it is otherwise required or authorised by law
- it will prevent or lessen a serious threat to somebody's life, health or safety or to public health or safety
- it is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities
- it is reasonably necessary to assist in locating a missing person
- it is reasonably necessary to establish, exercise or defend a claim at law
- it is reasonably necessary for a confidential dispute resolution process
- it is necessary to provide a health service
- it is necessary for the management, funding or monitoring of a health service relevant to public health or safety
- it is necessary for research or the compilation or analysis of statistics relevant to public health or public safety
- it is reasonably necessary for the enforcement of a law conducted by an enforcement body.

We do not usually send personal information out of Australia. If we are otherwise required to send information overseas, for example if sending a hard copy document or email containing an individual's personal information to an overseas client, or publishing information on the internet and it is accessed by an overseas recipient, or to an overseas contractor providing service for us or sub-

## PRIVACY AND CONFIDENTIALITY

contractor, we will take measures to protect your personal information. We will protect your personal information either by ensuring that the country of destination has similar protections in relation to privacy or that we enter into contractual arrangements with the recipient of your personal information that safeguards your privacy.

### **Security of Personal and Sensitive Information**

We take reasonable steps to protect the personal and sensitive information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.

These steps include password protection for accessing our electronic IT system, securing paper files in locked cabinets and physical access restrictions. Only authorised personnel are permitted to access these details.

We provide for security of our IT systems and information, which is documented in the ICT Information Management and Security policy.

Personal and sensitive information may be stored in databases that are located outside of Australia. Where this is the case these facilities are used for storage purposes only and we maintain full control of all data. We ensure that all contractual relationships for the storage of data complies with Australian law and meets the cloud computing guidelines established by the Australian Government Information Management Office.

When the personal information is no longer required, it is destroyed in a secure manner, de-identified, or deleted according to our documentation, data and records control procedure, and respective archiving and disposal procedures. These are listed in the References section.

### **Quality of Personal Information**

We take reasonable steps to ensure that the personal information collected, used and disclosed in having regard to the purpose or use of the disclosure is accurate, up to date and complete.

Please notify us if your personal details or information have changed so we can update our records. We provide mechanisms to facilitate the update of personal details and information through service delivery practices, which may include website, electronic, letter/form, verbally, or through individual service delivery review practices.

### **Access to and Correction of Personal Information**

If an individual requests access to the personal information we hold about them, or requests that we change that personal information, we will allow access or make changes unless we consider that there is a sound reason under the Privacy Act or other relevant law to withhold the information, or not make the changes.

Requests for access and/or correction should be made to the Privacy Officer (details of which are set out in the Contact section of this policy). For security reasons, you will be required to put your request in writing and provide proof of your identity. This is necessary to ensure that personal information is provided only to the correct individuals and that the privacy of others is not undermined.

If the information is unable to be corrected when an individual makes a request the reason for such refusal will be provided in writing to the individual and information about the complaints mechanism provided within a reasonable period.

## PRIVACY AND CONFIDENTIALITY

In the first instance, we will generally provide a summary of the information held about the individual. It will be assumed (unless told otherwise) that the request relates to current records. These current records will include personal information which is included in our databases and in paper and electronic files, and which may be used on a day to day basis.

We will provide access by allowing you to inspect, take notes or print outs of personal information that we hold about you. If personal information (for example, your name and address details) is duplicated across different databases, we will generally provide one printout of this information, rather than multiple printouts.

We will take all reasonable steps to provide access or the information requested within 14 days of your request. In situations where the request is complicated or requires access to a large volume of information, we will take all reasonable steps to provide access to the information requested within 30 days.

We may charge you reasonable fees to reimburse us for the cost we incur relating to your request for access to information, including in relation to photocopying and delivery cost of information stored off site. For current fees, please contact the Privacy Officer.

If an individual is able to establish that personal information we hold about her/him is not accurate, complete or up to date, we will take reasonable steps to correct our records.

Access will be denied if:

- the request does not relate to the personal information of the person making the request
- providing access would pose a serious threat to the life, health or safety of a person or to public health or public safety
- providing access would create an unreasonable impact on the privacy of others
- the request is frivolous and vexatious
- the request relates to existing or anticipated legal proceedings
- providing access would prejudice negotiations with the individual making the request
- access would be unlawful
- denial of access is authorised or required by law
- access would prejudice law enforcement activities
- access would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of Spinal Life Australia
- access discloses a 'commercially sensitive' decision making process or information; or
- any other reason that is provided for in the APP's or in the Privacy Act.

If we deny access to information we will set out our reasons for denying access. Where there is a dispute about your right of access to information or forms of access, this will be dealt with in accordance with the complaints procedure set out below.

### Complaints Procedure

If you have provided us with personal and sensitive information, or we have collected and hold your personal and sensitive information, you have a right to make a complaint and have it investigated and dealt with under this complaints procedure.

**PRIVACY AND CONFIDENTIALITY**

If you have a complaint about our privacy practices or our handling of your personal and sensitive information, please contact our Privacy Officer (details of which are set out in the Contact section of this policy).

All complaints will be logged on our complaints register database.

A privacy complaint relates to any concern that you may have regarding our privacy practices or our handling of your personal and sensitive information. This could include matters such as how your information is collected or stored, how your information is used or disclosed or how access is provided to your personal and sensitive information.

The goal of this policy is to achieve an effective resolution of your complaint within a reasonable timeframe, usually 30 days or as soon as practicable.

However, in some cases, particularly if the matter is complex, the resolution may take longer.

Once the complaint has been made, we will try to resolve the matter in a number of ways such as:

- Request for further information: we may request further information from you. You should be prepared to provide us with as much information as possible, including details of any relevant dates and documentation. This will enable us to investigate the complaint and determine an appropriate solution. All details provided will be kept confidential.
- Discuss options: we will discuss options for resolution with you and if you have suggestions about how the matter might be resolved you should raise these with our Privacy Officer.
- Investigation: where necessary, the complaint will be investigated. We will try to do so within a reasonable timeframe. It may be necessary to contact others in order to proceed with the investigation. This may be necessary in order to progress your complaint.
- Conduct of our employees: if your complaint involves the conduct of our employees we will raise the matter with the employee concerned and seek their comment and input in the resolution of the complaint.
- The complaint is substantiated: if your complaint is found to be substantiated, you will be informed of this finding. We will then take appropriate agreed steps to resolve the complaint, address your concerns and prevent the problem from recurring.
- If the complaint is not substantiated, or cannot be resolved to your satisfaction, but this Privacy and Confidentiality policy has been followed, we may decide to refer the issue to an appropriate intermediary. For example, this may mean an appropriately qualified lawyer or an agreed third party, to act as a mediator.
- At conclusion of the complaint, if you are still not satisfied with the outcome you are free to take your complaint to the Office of the Australian Information Commissioner at [www.oaic.gov.au](http://www.oaic.gov.au).

We will keep a record of your complaint and the outcome.

**PRIVACY AND CONFIDENTIALITY**

We are unable to deal with anonymous complaints. This is because we are unable to investigate and follow-up such complaints. However, in the event that an anonymous complaint is received we will note the issues raised and, where appropriate, try to investigate and resolve them appropriately.

We have policies and procedures in place to deal effectively with complaints. These processes are documented in the References section of this document.

**Part B – Personal Information Handling Practices in Relation to Functions or Activities****Contact Lists*****Purpose***

We maintain contact lists which include contact information about individuals who may have an interest in our services. We use these contact lists to distribute information about our services, programs, activities, publications, or for donation campaigns, community fundraising events and sponsors, or marketing campaigns for fundraising activities.

***Collection***

It is our usual practice to collect personal information in contact lists directly from individuals, for example, where they have asked to be added to a contact list or subscriber list.

Sometimes we collect personal information from a third party organisation or from a publicly available source such as a website or telephone directory. We usually only collect personal information in this way if the individual would reasonably expect us to, or has given their consent. For instance, we might collect this information if we thought that the individual (or the organisation they work for) would like to receive information about the services we are carrying out, what is happening at Spinal Life Australia, or that they might be likely to consider information about spinal injuries prevention programs, or disability care or support useful in the work that they do, or to participate in a fundraising activity. We would only contact this individual in their work capacity, or by the details provided to us in a particular list or where the individual has subscribed to.

***Use and disclosure***

We only use personal information in contact lists for the purpose of managing stakeholder relations. We do not give personal information about an individual to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

***Direct marketing*** - In activities related to direct marketing where an individual would not reasonably expect his or her personal information to be used for direct marketing, or the information was collected from a third party, we may only use or disclose the information for the purpose of direct marketing if the individual has consented to the use and disclosure for that purpose, or where it is impracticable to obtain their consent we will provide a simple means for the individual to opt out of receiving information from us and the individual has not opted out. In each direct marketing communication, a prominent statement will be displayed which tells the individual that he or she may request to no longer receive direct marketing and where no request is made it will be assumed that consent is agreed.

## PRIVACY AND CONFIDENTIALITY

Consent of the individual before using or disclosing sensitive information for the purpose of direct marketing will be obtained. It is not normal practice to use sensitive information for direct marketing purposes.

### **Data quality**

We maintain and update personal information in our contact lists when we are advised by individuals that their personal information has changed. We also regularly audit contact lists to check the currency of the contact information. We will remove contact information of individuals who advise us that they no longer wish to be contacted.

### **Data security**

The personal information in the contacts lists is stored in either password protected electronic media or locked cabinets in paper form. When no longer required, personal information in contact lists is destroyed in a secure manner, de-identified, or deleted according to our documentation, data and records control procedure, and respective archiving and disposal procedures. These are listed in the References section.

Routine access to contact lists is limited to the database operators who have responsibility for maintaining the contact lists. Other staff members have access to the personal information in contacts lists on a need to know basis.

### **Access and correction**

For information about how to access or correct personal information in our contacts lists see 'Access to and Correction of Personal Information' in Part A of this document.

## **Public Awareness and Education Files**

### **Purpose**

The purpose of public awareness and education files is to record details of public awareness and educational activities. For example, contact with the media, media releases, clips, speeches and speaking engagements, educational message videos, event management, competition entries, surveys, community awards, community service announcements, newsletters, interviews, promotional collateral, education resources, print materials, reports, photography and publication preparation etc.

The limited personal information in public awareness and education files relates to organisations, individuals, media representatives, event attendees, service providers and event calendar listings which appear on our website and in publications produced by us.

### **Collection**

It is our usual practice to collect personal information in public awareness and education files directly from individuals. Sometimes we may collect personal information from an individual's representative or from publicly available sources such as websites, telephone directories, or through subscribed news media agents.

### **Use and disclosure**

We only use the personal information in public awareness and education files for the purposes of undertaking public awareness and education initiatives and managing public relations. Consent is sought for use of photos, filming and testimonials in publications.

**PRIVACY AND CONFIDENTIALITY**

The personal information on public awareness and education files is not disclosed to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

**Data quality**

We maintain and update personal information in our public awareness and education files as necessary, or when we are advised by individuals that their personal information has changed.

**Data security**

Public awareness and education files are stored in either password protected electronic media or in locked cabinets in paper form. When no longer required, personal information in public awareness and education files is destroyed in a secure manner, de-identified, or deleted in accordance with our documentation, data and records control procedure, and respective archiving and disposal procedures. These are listed in the References section.

The following departments' management and coordinators have access to public awareness and education files on a need to know basis:

- Communications, Fundraising and Injury Prevention Programs
- Community Development
- Executive office and corporate services staff.

**Access and correction**

For information about how to access or correct personal information in public awareness and education files see 'Access to and Correction of Personal Information' in Part A of this document.

**Enquiries****Purpose**

We hold enquiry lists which include contact information about individuals who may have an interest in our services. We use these contact lists to enable us to make contact with the person and assist them with their enquiry, to prioritise their enquiry or service, and/or make the most appropriate referral if we are unable to provide a service.

**Collection**

It is our usual practice to collect personal information with the enquiry directly from individuals, for example, where they have asked about a service, wish to access or register for a service, or to learn more about the organisation, or to make contact with a particular department or service officer.

We usually only collect personal information in this way if the individual would reasonably expect us to, or has given their consent to direct the enquiry to the most relevant person or department of the organisation

Information which may be collected includes name, email address, phone number and message. We can receive enquiries through the website, by email, or by phone.

## PRIVACY AND CONFIDENTIALITY

Some more complex enquiries in relation to particular service access may have personal or sensitive information recorded on a form, which will be prioritised as part of the service access procedures of the service. Permission from the individual will be sought when collecting sensitive information.

### ***Use and disclosure***

We only use personal information in enquiry lists for the purpose of attending appropriately to your enquiry. We do not give personal information about an individual to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

### ***Data quality***

We maintain and update personal information in our enquiry lists or forms when we are advised by individuals that their personal information has changed.

### ***Data security***

The personal information in the enquiry lists is stored in either password protected electronic media, or locked cabinets in paper form. When no longer required, personal information in contact lists is destroyed in a secure manner, de-identified, or deleted according to our documentation, data and records control procedure, and respective archiving and disposal procedures. These are listed in the References section.

Routine access to enquiries is limited to the database operators who have responsibility for following up with the enquiry. Other staff members have access to the personal information in contacts lists on a need to know basis.

### ***Access and correction***

For information about how to access or correct personal information in our enquiry lists or forms see 'Access to and Correction of Personal Information' in Part A of this document.

## **Visitors and contractors**

### ***Purpose***

Visitors and contractors who present at Spinal Life Australia are identified in order to facilitate services and communications with in the organisation departments and allow visibility of authorisation to the premises for the purpose of the business and provide evidence of participation of that activity. This may include attending meetings, interviews, and events, training sessions, or providing a contracted service.

### ***Collection***

Visitors provide their name, company name, meeting with/responsible to, date, and signature, which allow the authorisation and validation of their participation and understanding of conditions of entry, safety information and returns.

Authorised contractors are requested to provide their name, company name, type of contractor, phone, vehicle registration no., key/access cards issued, the work area, and description of work. ID and/or prescribed licence are checked, safety induction undertaken and permits in order recorded, which is signed by the contractor for authorisation and returns following the completion of the work.

### ***Use and disclosure***



## PRIVACY AND CONFIDENTIALITY

We only use personal information provided in the sign in registers for the purpose providing authorised access, facilitating the communication with the relevant department personnel and checking the validity of the visit and/or licensing permits.

### **Data quality**

The individual completes the register entry. If there is an inaccuracy, correction will occur when advised by the person of the change required.

### **Data security**

The personal information is stored as a hard copy in the register, and locked away when not in use. When no longer required, registers are destroyed in a secure manner, according to our records, documents and data control, archiving and disposal procedures. These are listed in the References section.

### **Access and correction**

For information about how to access or correct personal information in our registers or forms see 'Access to and Correction of Personal Information' in Part A of this document.

## **Surveillance cameras (CCTV)**

### **Purpose**

CCTV cameras are used to collect footage of activity, vehicles and of individuals who may be identifiable or reasonably identifiable surrounding the office facility and car park. The purpose is to monitor and notify staff of people within the building premises of visitors, taxis, safety assistance, and for security purposes to identify incidents which may occur in this area.

### **Collection**

Cameras are clearly visible around the perimeter of the building and signage displays the use of security systems installed. Footage is recorded and held for a defined period of time.

### **Use and disclosure**

Authorised staff only use information collected for monitoring of the premises and intelligence gathering. The information collected may be used for the secondary purpose of disclosure to an enforcement body or where the collection is required or authorised by or under an Australian law or a court/tribunal order, or other exceptions listed in the Privacy Act.

### **Data quality**

Individuals may or may not be identifiable due to external variables.

### **Data security**

Footage is stored for a defined period of time in secure IT systems and then automatically overwritten.

### **Access and correction**

For information about how to access or correct personal information in our registers or forms see 'Access to and Correction of Personal Information' in Part A of this document.

**PRIVACY AND CONFIDENTIALITY****Part C – Confidentiality Practices****Confidentiality Agreement**

Spinal Life Australia manages the risk of breaches to privacy through complying with the APP's and Privacy Act. In addition to the processes implemented surrounding Part A and Part B of this policy, we have implemented confidentiality management practices, which are layered over the privacy of personal information obligations.

All employees, volunteers and contractors understand their obligations for privacy and intellectual property protection through validation of a signed Confidentiality Agreement, prior to the commencement of work. The agreement serves to keep confidential all information and material he/she may have access to while employed/engaged by the organisation, and after the period of employment ceases or has been altered.

The worker acknowledges and accepts that during the course of their employment they will have access to information or be exposed to business practices which are to remain the property of Spinal Life Australia.

Confidential information, including others' personal information, and all records, documents, accounts, correspondence and papers of every description (including copies/extracts) whether relating to the affairs or business or not, are solely for the purpose of carrying out tasks and obligations of employment.

The worker acknowledges on signing the agreement that he/she will:

- demonstrate respect for the rights to privacy of individuals as a legal obligation and in accordance with the organisation's Privacy and Confidentiality policy and related policies and procedures
- treat as confidential and not disclose, record, reproduce, duplicate, use, discuss, permit the use of or otherwise make available the confidential information to any party without the prior written consent of Spinal Life Australia and in accordance with legal obligations. These matters include but are not restricted to:
  - details or information about members, clients/beneficiaries, donors, business partners, contractors, customers, suppliers or employees (stakeholders)
  - details of wages, salaries, prices, or financial information
  - details of work processes, trade secrets, intellectual property, governance and management information.
- fully protect the confidentiality of all confidential information, including communications received or distributed electronically (e.g. Email, SMS, Messaging) or in hard copy from unauthorised access or disclosure
- not utilise, in any manner or form, the confidential information in an unauthorised form, and not acquire any proprietary interest or any other right to use the confidential information
- not utilise social networking sites (eg. Facebook, Twitter, My Space) to discuss client/employee/member and organisation matters
- acknowledge that all copyright, design, patent and trademark rights, eligible layout rights and any other intellectual property rights in respect of any material, resources, programs, ideas, reports or any other articles or thing, which is created or devised by he/she during

## PRIVACY AND CONFIDENTIALITY

the course of employment are and remain the property of Spinal Life Australia, or its stakeholders.

- management will be advised where he/she realises a breach in disclosure has occurred
- management will be immediately notified in the event he/she is required to make a disclosure of any private or confidential information in any proceedings before any court, tribunal or other body, or where required to make a disclosure pursuant to any law
- all confidential information in his/her possession, power or control will be immediately returned to Spinal Life Australia when employment ceases and that any copies of information, including any personal information about individuals will be securely destroyed, de-identified or deleted where these cannot be physically returned.
- any breach of confidentiality could result in disciplinary action which may include instant dismissal.

### Induction and training

Induction training is provided to all employees and volunteers at commencement of employment which includes familiarisation with the Privacy and Confidentiality policy, procedures and legislation. Resources are provided to outline what privacy and confidentiality means to the worker in their role. Opportunities to attend to professional development and/or refresher training in privacy and confidentiality are provided.

### Risk management

A privacy risk review is undertaken annually in accordance with the Risk Management Plan. The risk assessment reviews IT systems security and potential for privacy and security breaches. Processes are in place across operations to manage privacy and security risk and what happens if a breach has occurred and how it will be responded to and managed.

### Evaluation and Review

#### ***Changes to this Privacy and Confidentiality Policy***

Spinal Life Australia reserves the right to review, amend and/or update this policy from time to time.

We aim to comply with the APPs and other privacy requirements required to be observed under State or Commonwealth Government contracts. If further privacy legislation and/or self-regulatory codes are introduced or our Privacy and Confidentiality policy is updated, we will summarise any substantial modifications or enhancements in this section.

Policy reviews are conducted in accordance with the Continual Improvement procedure and our Documentation, Data and Records Control procedure.

### Contact Details

#### **How to contact us**

Individuals can obtain further information in relation to this Privacy and Confidentiality policy, or provide any comments, by contacting us in a variety of ways:

#### **Brisbane office**

109 Logan Road  
WOOLLOONGABBA QLD 4102  
PO Box 5651  
WEST END QLD 4101  
Ph: 1300 774 625

#### **Townsville office**

488 Ross River Road  
TOWNSVILLE QLD 4814  
PO Box 618  
AITKENVALE BC QLD 4814  
Ph: 1300 774 625

#### **Cairns office**

Unit 1, 325-327 Sheridan St  
NORTH CAIRNS QLD 4870  
PO Box 452  
NORTH CAIRNS QLD 4870  
Tel: 1300 774 625

**PRIVACY AND CONFIDENTIALITY**

Fax: 1300 655 885  
[enquiries@spinal.com.au](mailto:enquiries@spinal.com.au)

Fax: 1300 655 885  
[nqenquiries@spinal.com.au](mailto:nqenquiries@spinal.com.au)

Fax: 1300 655 885  
[nqenquiries@spinal.com.au](mailto:nqenquiries@spinal.com.au)

**Website** – Contact us, or see our Feedback section: <http://www.spinal.com.au/>  
**Privacy Officer** – [privacy@spinal.com.au](mailto:privacy@spinal.com.au)

**Assisted Contact Options**

National Relay Service (NRS)

If you are deaf, have a hearing or speech impairment you can contact us via the NRS

**TTY - 133 677 then ask for 1800 810 513**

**Voice - 1300 555 727 then ask for 1800 810 513**

Find out more about registering with the NRS

**Definitions**

**Online Users** – refers to anyone that accesses the Spinal Life Australia website.

<http://www.spinal.com.au/>

**Personal Information** – as defined by the Privacy Act 1988 (as amended) is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not.

**Sensitive Information** – as defined by the Privacy Act 1988 (as amended) is information or opinion (that is also personal information) about an individual's 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, or health, genetic, biometric information or biometric templates, that is also personal information.

**Health information** - is defined to mean:

- information or an opinion, that is also personal information, about:
  - o the health or a disability (at any time) of an individual, or
  - o an individual's expressed wishes about the future provision of health services to him or her, or
  - o a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a health service, or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. Other types of genetic information that are not health information fall within the definition of 'sensitive information'.

**Health service** - is defined to mean:

- an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
  - o to assess, record, maintain or improve the individual's health, or
  - o to diagnose the individual's illness or disability, or
  - o to treat the individual's illness or disability or suspected illness or disability, or
- the dispensing or prescription of a drug or medicinal preparation by a pharmacist.

## PRIVACY AND CONFIDENTIALITY

**Reasonably identifiable** - is defined in the Act. Whether an individual is 'reasonably identifiable' from particular information will depend on considerations described in the Act.

**Deceased person** - the definition of 'personal information' refers to information or an opinion about an 'individual.' An 'individual' means 'a natural person'. The ordinary meaning of 'natural person' does not include deceased persons.

**Normal business practices** - An APP entity does not need to include in its description internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.

**The website** – means Spinal Life Australia's website. <http://www.spinal.com.au/>

### References

- Archiving procedure
- Authorities to Release forms
- Client Images Photograph procedure
- Confidentiality Agreement
- Code of Conduct
- Code of Ethics
- Deed of Confidentiality and Intellectual Property
- Documentation, Data and Records Control procedure
- Events policy
- Feedback, Satisfaction, Grievance, Complaints and Appeals policy
- Fundraising policy
- Health, Safety and Wellbeing policy
- Human Resource Management policy
- ICT Code of Practice for Users
- ICT Information Management and Security policy
- Managing Privacy – User Guide for Handling Personal Information, manual
- Member Networks Member Contact List procedure
- Photo and Filming Consent forms
- Privacy and Confidentiality procedure
- Privacy Compliance Checklist – self assessment
- Privacy Notice and Consent forms
- Privacy Statement - general
- Records Management policy
- Risk Management policy
- Risk Management Plan procedure
- Service Access policy
- Service Commitment policy
- Service Planning and Management policy
- Register of Authorised Contractors
- Visitor Sign-in Pass – and Fire Register
- Website policy
- Workplace Health and Safety Management policy
- Workplace Surveillance procedure

## PRIVACY AND CONFIDENTIALITY

- ADMA Code of Practice
- APP Guidelines (OAIC) <https://www.oaic.gov.au>
- Information Privacy Act, 2009 (Qld)
- Privacy Act 1988 (C'th)
- Privacy & Cloud Computing for Australian Government Agencies – Better Practice Guide Feb 2013 V1.1

### **Quality Management System Standards**

#### **HSQF – Human Services Quality Framework**

- 1 – Governance and Management (1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7)
- 2 – Service Access (2.1, 2.2, 2.3)
- 3 – Responding to Individual Need (3.1, 3.2, 3.3, 3.4, 3.5)
- 4 – Safety, Well-being and Choice (4.1, 4.2, 4.3, 4.4, 4.5)
- 5 – Feedback, Complaints and Appeals (5.1, 5.2, 5.3, 5.4)
- 6 – Human Resources (6.1, 6.2, 6.3, 6.4, 6.5)

#### **NSDS – National Standards for Disability Services**

- 1 – Rights (1.1, 1.2, 1.3, 1.5, 1.6, 1.7, 1.8, 1.9)
- 2 – Participation and Inclusion (2.2, 2.3, 2.4, 2.5)
- 3 – Individual Outcomes (3.1, 3.2, 3.3, 3.5)
- 4 – Feedback and Complaints (4.1, 4.2, 4.3, 4.4, 4.5, 4.6)
- 5 – Service Access (5.1, 5.2, 5.3, 5.6, 5.7)
- 6 – Service Management (6.1, 6.3, 6.4, 6.5, 6.6, 6.7)

#### **VHC Guidelines**

- Objective 5 – Privacy, confidentiality and access to personal information  
Objective 6 - Complaints and disputes

#### **CCCS - Community Care Common Standards (hacc)**

- 1 - Effective management (1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7)
- 2 - Appropriate access and service delivery (2.1, 2.2, 2.3, 2.4, 2.5)
- 3- Service user rights and responsibilities (3.1, 3.2, 3.3)

#### **ISO9001:2015 – Quality Management System**

- 4 – Context of the organisation (4.1, 4.2, 4.3, 4.4)
- 5 – Leadership (5.1, 5.2, 5.3)
- 6 – Planning (6.1, 6.2, 6.3)
- 7 – Support (7.1, 7.2, 7.3, 7.4, 7.5)
- 8 – Operation (8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7)
- 9 – Performance evaluation (9.1, 9.2, 9.3)
- 10 – Improvement (10.1, 10.2, 10.3)

This policy has been approved and authorised for distribution in accordance with the Documentation, Data and Record Control procedure and Continual Improvement procedure.

**Name:** Michael Powell , CEO

**Signature:**



**Date:** 13/10/2016