Southern Peninsula Community Support
Privacy Statement

Southern Peninsula Community Support Inc. (referred to as SPCS, we, us or our) is strongly committed to protecting the privacy of its members, clients, supporters and donors, volunteers, staff and all members of the public who deal with SPCS, and has implemented the SPCS Privacy Policy, which includes this Privacy Statement, to provide you with information about how we collect, hold and use personal information you provide to us.

SPCS may, from time to time, review and update our Privacy Policy and/or our Privacy Statement, including to take into account new laws, regulations, practices and technology. All personal information held by the SPCS will be governed by our most recent Privacy Policy (including this Privacy Statement). We will post on our website that changes have been made to the Privacy Policy and publish on our website the effective date when the Privacy Policy is updated. From time to time, we may use the personal information already collected to identify new products/services we believe may be of interest to you or use personal information in new ways. We will generally only do this where we are permitted to do so under the relevant privacy laws.

To the extent applicable, SPCS will comply with the relevant Acts covering the legitimate collection and handling of an individual's personal information. The relevant Acts are:

- Privacy and Data Protection Act 2014 (Vic) Click here
- Health Records Act 2001 (Vic) Click Here
- Freedom of Information Act 1982 (Vic) Click Here
- Public Records Act 1973 (Vic) Click Here
- Privacy Act 1988 (Cth) including the Australian Privacy Principles (APPs) in the Act and the Notifiable Data Breaches (NDB) scheme of the Privacy Act Click here

Risk Management

SPCS takes a risk management approach to collecting, storing, using and sharing your personal information and data. We know the risks and take steps to mitigate them as the most important element of best practice charity governance. Our Board is highly aware of and sensitive to its legal responsibility in managing personal information and data. Where a data breach occurs, and meets applicable harm thresholds, SPCS follows the mandatory data breach notification procedures in accordance with the guidance of the relevant regulator.

What personal information does SPCS collect?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

This includes information such as:

- name, including the name of an authorised parent, guardian, carer or other representative who you have nominated as your representative,
- date of birth and gender,
- the name, address and contact details of your organisation or business (if applicable),
- contact information (such as a home address, email address and phone number),
- credit/debit card and bank account information,
- signatures
- employment details
- details of products or services purchased or received from SPCS and SPCS suppliers (such as products from Emergency Relief programs, case management and support services, Outreach programs, fundraising activities, education, peer support and networking and

information services),
- details of service and product preferences
- details of the products or services purchased, received or in which individuals have participated (such as the name and date of the fundraising activity or professional development/training program),
- health information and other sensitive information (as set out in further detail under "Health information and other sensitive information", below), and
- other information about your history with, or relationship to our services.

Whose personal information does SPCS collect?

SPCS collects personal information from and/or about people who are connected to its operations and activities – including:

- employees,
- volunteers,
- donors,
- supporters,
- customers,
- clients,
- recipients of support services,
- participants in advocacy campaigns or promotion projects,
- welfare sector professionals, and
- suppliers and service providers.

We also collect information about you if you are a user of our website.

How does SPCS collect your personal information?

Where possible, SPCS will collect your personal information directly from you. This may be:

- in person e.g. attend an Emergency Relief interview, when you make a donation, drop off goods or attend an event or our workplace,
- on the telephone e.g. if you contact SPCS by phone for Emergency Relief assistance or for case management support,
- by mail, e.g. if you mail in information as part of a support service, if you complete a survey, if we receive a donation from you,
- online e.g. to donate via an online donation portal or register to volunteer on our volunteer portal.
- social media, e.g. you ‘Like’ or ‘Follow’ an SPCS page,
- SMS, e.g. you reply to a text requesting a donation,

Where it is unreasonable or impracticable to collect personal information about you directly from you, we may also collect your personal information from third parties such as:

- contractors (including fundraising service providers),
- list vendors,
- parent/carer
- health professionals, and
- social and community workers.

Where we engage with you multiple times over a short period in relation to the same matter, we may not provide you with a separate notice about privacy each time we engage with you.

Why does SPCS collect your personal information?

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

- Support services: to provide you with information, our products and support services, and to evaluate and report on these services.

- Service partners and their staff.
- Marketing: to communicate with you about donations, products, services, campaigns, causes and events.
- Fundraising operations: to administer fundraising events (including to process receipts and conduct those events) and to communicate with you in relation to those events;
- Dealings with suppliers and medical and health professionals: to administer our dealings and potential dealings with suppliers of our products and services, including medical and health professionals.
- Promotion of support services: to provide you with information about risk factors of inadequate incomes to cover the cost of living and housing, and to seek your support for campaigns.
- Employment: to process any job application submitted by you, conduct employment activities with staff and for other employment-related purposes.
- Volunteering and other support: to enable you to assist us with volunteering, community fundraising, advocacy and other activities where we seek the community's assistance; and
- Other issues: communicating with you in relation to our operations, activities and objectives, to verify your identity, to improve and evaluate our programs and services and to comply with relevant laws.

In some cases, SPCS may collect your personal information as part of our responsibilities of receiving government funding e.g. we are part of the Community Information Support Victoria (CISVic) consortium that receives Emergency Relief funds from Department of Social Security (DSS). We do from time to time receive other funds from government that includes federal, state and local government.

In those circumstances, your personal information will be collected, used and disclosed by SPCS as part of a secure Client Management System (CMS). SPCS will use that information to manage its support to you through its various programs. CISVic will have access to the CMS to manage the safe, effective running of the CMS. When reporting to any level of government only aggregated, de identified information is provided.

We will provide you with a collection notice which explains the primary purpose for which we are collecting your personal information.

Unless required or authorised by law to use or disclose your personal information, SPCS will not use or disclose personal information that was provided for a particular purpose for other purposes unless:

- (a) you have consented to the use or disclosure of the information for that other purpose; or
- (b) the purpose for which the information is used or disclosed is directly related to the purpose for which the personal information was obtained.

If you would like to change any consents you previously provided us, or you have any questions about how we use and disclose your personal information, please contact SPCS using any of the details set out at the end of this Privacy Statement.

Health information and other sensitive information

As part of administering SPCS's services and in our role as an employer to comply with our legal obligations, and depending on who you are, we may collect health information and other sensitive information about you.

For example, we may collect medical history information from you, if you are participating in any of our support programs. Sensitive information is defined by law as the following type of information:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or associations;
- philosophical beliefs;
- memberships of a professional or trade association, or of a trade union;
- sexual orientation;
- criminal record;
- health information;

- genetic information;
- biometric information; or
- biometric templates.

We will only collect these types of information if it is necessary to deliver a service to you and you have specifically consented to the collection of that information or where we are otherwise permitted by applicable privacy laws to do so.

COVID-19: given the impacts of COVID-19, the nature of the services SPCS provides, its role as an employer and the mandatory vaccination orders and directions that are issued from time to time, we may request evidence and collect the vaccination status of all individuals who work or attend at our premises or attend events, functions or fundraisers organised by us, including employees, contractors, and volunteers.

What happens if you don't provide all the information requested?

You are free to provide (or not provide) any information you choose. However, if you do not provide some or all of the personal information requested, we may not be able to offer you services or products, allow you to participate in SPCS's programs, events or fundraisers, or provide you with information about our cause, events, programs and projects. For our employees, contractors, volunteers, if you do not provide some or all of the personal information requested, this may affect your application or ability to work with us.

Collection of your COVID-19 vaccination status: if you do not provide the information we request about your status we may not be able to ensure that we remain in compliance with the mandatory vaccination orders and directions that are issued from time to time and meet our obligation to maintain a safe workplace, which may affect your employment status with SPCS.

Website usage information and cookies

When you access our website, we may use software embedded in our website (such as Javascript) and we may place small data files (or cookies) on your computer or other device to collect information about which pages you view and how you reach them, what you do when you visit a page, the length of time you remain on the page, and how we perform in providing content to you.

A cookie does not identify individuals personally, but it does identify computers. You can set your browser to notify you when you receive a cookie, and this will provide you with an opportunity to either accept or reject it in each instance. If you disable the use of cookies on your browser or remove or reject specific cookies from our website or linked sites, then you may not be able to gain access to all of the content and facilities on those websites.

We may gather your IP address as part of our business activities and to assist with any operational difficulties or support issues with our services. This information does not identify you personally.

How we handle email and "Contact us" forms and messages

SPCS may preserve the content of any email, completed "Contact us" form or other electronic message or form that we receive. Any personal information contained in those messages will only be used or disclosed in accordance with this SPCS Privacy Statement. The message content may be monitored by our service providers or SPCS employees for purposes including trouble shooting, compliance, auditing and maintenance, or where email abuse is suspected, which means that your personal information may be disclosed to third party service providers.

Links

SPCS website and its social media channels may, from time to time, contain links to the websites and social media sites/profiles of other organisations or individuals which may be of interest to you. These third-party websites or profiles themselves may facilitate collection of information by those third parties, through your interaction with the websites or profiles and sometimes even if you do not interact directly

with them. We are not responsible for the technical operation of these websites or profiles or the collection and use practices of the relevant third parties. Linked websites and social media sites/profiles are responsible for their own privacy practices and you should check those websites and social media sites/profiles for their respective privacy policies to understand their privacy practices and options they may make available to you in relation to their collection of your personal information.

Social media

SPCS uses a range of social media accounts to inform, engage, communicate with and learn from stakeholders and the wider community. SPCS's social media team may choose to follow organisations and individuals involved with, or actively discussing relevant issues. Individuals and organisations choosing to follow SPCS may be followed, friended or your posts shared or connected to in return, but SPCS only contacts individuals who have initiated the communication through social media.

You may request that SPCS stop following you by a request to the account, emailing admin@spcsic.org or by blocking SPCS's accounts using the block function in the relevant social media account. You are reminded that social media operates in a public space on the internet and most interactions are publicly viewable and searchable over time. For more information on how best to manage your interactions visit the social media account's host website (e.g. www.facebook.com).

The SPCS social media team responses should be considered as comparatively informal, especially when they are dealing with enquiries and direct messages sent via our social media accounts. SPCS has formal procedures for providing support and can only respond to emails, post and phone.

The SPCS social media team periodically monitors accounts during business hours (Australian Eastern Time). The accounts may also be intermittently monitored outside business hours subject to staff availability; we reserve the right to remove any posts not complying with acceptable use.

Third party sites or profiles linked from our social media accounts are not controlled, maintained or endorsed by SPCS. To the extent permitted by law, SPCS is not responsible or liable for any content posted on or uploaded to our social media accounts by a user or any content on third party sites linked to by our social media accounts.

Opting out of direct marketing communications

From time to time, SPCS may send you information, including promotional material, about us, our products and services, fundraising activities and events. You consent to us using your personal Information for sending you such information, now and in the future. You also consent to us sending you such information by means of direct mail, SMS, telephone, email or messaging and/or notifications that are part of online Apps.

If you do not wish to receive or if you wish to modify how you receive or how much direct marketing communication you receive from us, please contact us in any of the ways set out under "Contact, complaints and further information", below.

To whom does SPCS disclose your personal information?

- We may need to disclose your personal information to others in order to carry out our activities and comply with our legal obligations, including in connection with the purposes described in this Privacy Statement.
- If you are a client of our support services, we will only disclose your personal information externally with your written informed consent, or verbal authority by phone unless required by law or if we believe there is a risk to your, or someone else's, health and safety.
- Depending on the nature of your engagement with us, SPCS may disclose your personal information to: External support services: to health care professionals, lawyers, other professionals, counsellors, funders, financiers, co-ordinators, volunteers, service providers, agencies and not-for-profits that provide support services.
- Third parties for marketing purposes: we may provide your contact details to other like-minded organisations to contact you with information that may be of interest to you, where you have

consented to us doing so.

- Contractors and service providers: who perform services on our behalf, such as mailing houses, printers, information technology services providers (including offshore cloud computing service providers), database contractors and telemarketing agencies.
- Corporate partners: who may wish to provide special offers to SPCS supporters.

Where is your personal information stored?

Your personal information will be stored on a password protected electronic database, which may be an SPCS database, a database maintained by a cloud hosting service provider or other third-party database storage or server provider. Backups of electronic information are currently stored with cloud-based security providers.

Hard copy information is generally stored in our offices, which are secured to prevent entry by unauthorised people. It may be stored for a time with a third party for specific purposes, for example at a mailing house. Any personal information not actively being used is archived, usually for 7 years, after which time it is securely destroyed.

Where personal information is stored with a third party, we have arrangements which require those third parties to maintain the security of the information. We take reasonable steps to protect the privacy and security of that information, but we are not liable for any unauthorised access or use of that information.

Your personal information will stay on the database indefinitely until you advise you would like it removed, unless we de-identify it or destroy it earlier in accordance with privacy law requirements.

Due to the complexity of SPCS's operations, your personal information may be stored simultaneously in more than one database or location.

We comply with the Payment Card Industry standards when handling payment card transactions. This means that we handle payment card information extremely securely while transactions are made, and do not retain payment card details afterwards.

Your direct debit or credit cards; or bank account details

We use Secure Socket Layer (SSL) certificates which is the industry standard for encrypting your credit card and debit card numbers, bank account details, your name and address so that it cannot be viewed by any third party over the internet. Your financial information is encrypted on our servers and access to this information is restricted to authorised SPCS staff or authorised personnel at supplier agencies.

Access to your personal information

SPCS will, upon your request, and subject to applicable privacy laws, provide you with access to your personal information that is held by us and where possible in the form in which you request it. However, we request that you identify, as clearly as possible, the type/s of information requested. We will endeavour to deal with your request to provide access to your personal information within 30 days and you agree we may charge you our reasonable costs incurred in supplying you with access to this information . If we refuse your request to access your personal information, we will provide you with reasons for the refusal where required by law.

Your rights to access personal information are not absolute and in certain circumstances, privacy laws dictate that we are not required to grant access such as:

- access would pose a serious threat to the life, safety or health of any individual or to public health or public safety.
- access would have an unreasonable impact on the privacy of other individuals.
- the request is frivolous or vexatious.
- denying access is required or authorised by a law or a court or tribunal order.

- access would be unlawful, or
- access may prejudice commercial negotiations, legal proceedings, enforcement activities or appropriate action being taken in respect of a suspected unlawful activity or serious misconduct.

Updating your personal information:

You may ask us to update or delete the personal information we hold about you at any time. We will take reasonable steps to verify your identity before granting access or making any corrections to or deletion of your information. We also have obligations to take reasonable steps to correct personal information we hold when we are satisfied that it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held. To assist us in this, you need to provide true, accurate, current and complete information about yourself as requested, and promptly update the information provided to us to keep it true, accurate, current and complete.

If you require access to, or wish to update your personal information, please contact us in any of the ways set out under "Contact, complaints and further information", below. We will generally not charge you for obtaining your information in an electronic format, but if you would like a hard copy of your information, you may be charged a reasonable fee to cover expenses incurred. We will use all our reasonable efforts to correct the information. You may be required to authenticate your identity by providing your personal information or the personal information of others, such as your authorised representative or the person for whom you are an authorised representative.

Anonymity or pseudonymity

Sometimes a person may deal with SPCS anonymously or by using pseudonyms, such as when making a general enquiry. The nature of these calls may be recorded for evaluation purposes (for example assessing the amount of aid given out).

However, in a number of circumstances SPCS will not be able to deal with people in this way for practical or regulatory reasons.

A donor may request to remain anonymous for publication or recognition purposes but generally speaking donations of a material nature must be identified to be used for a tax deduction.

Contact, complaints and further information

If you:

- have any questions in relation to the Privacy Policy, including this Privacy Statement or the information handling procedures of SPCS,
- wish to make a complaint regarding the treatment or a breach of your privacy,
- would like to access your personal information held by us,
- would like to opt out of direct marketing, or
- would like to correct your personal information held by us,

please contact the Privacy Officer in any of the following ways:

- By telephone: (03) 5986 1285
- By email: admin@spcsic.org
- By ordinary mail addressed to: Privacy Officer, Southern Peninsula Community Support, PO Box 91, Rosebud, VIC 3939

We may need you to provide more information about your concern. If your concern is bona-fide, we will investigate the issue and endeavour to provide you with a written response within 28 days of receipt of your written query. Sometimes we might not be able to provide you with a written response within the timeframe specified. If that is the case, we will contact you and explain the reason for the delay and give you a new timeframe for a written response.

If you are not satisfied with our response, please notify the Privacy Officer in writing. We can escalate your matter and review the response that you were given. This may involve an escalation to the next level of management or referral to the CEO. You may also direct your issue to the Office of the Australian Information Commissioner's website at:

www.oaic.gov.au/privacy/privacy-complaints/

You are entitled to make an anonymous complaint or inquiry in relation to the Privacy Policy (including this Privacy Statement) or your privacy rights. However, we may require you to identify yourself if required by law or if it is impracticable for SPCS to deal with your matter otherwise.

This Privacy Statement is reviewed in conjunction with SPCS's Privacy Policy

Date of Endorsement: **Oct. 2023**

Date Last Reviewed: **Oct. 2023**

Next Review Date: **Oct. 2025** or when necessary to take into account new laws, regulations, practices and technology.