



SBDC Privacy Policy



Table of Contents

1. Purpose	3
2. Scope	3
3. Policy Definitions	4
4. Policy Statement	5
5. Disclosure of Personal Information	5
6. Information provided by third parties	6
7. Updates and access	6
8. Principles	6
9. Guidelines	9
10. Personal information we collect and hold	10
11. How we secure personal information	14
12. Roles and Responsibilities	14
Employees	14
Managers and Senior Leadership Team	14
Executive Leadership Team	15
Board	15
Information Technology	15
RACI Table	16
13. Relevant Legislation	16
14. Related Policies and Procedures	16
15. Relevant forms	17

1. Purpose

The purpose of the Small Business Development Corporation (SBDC) Privacy Policy (Policy) is to provide details on the requirements for all Board members and staff (including contracted personnel/companies) in keeping, maintaining, and using personal details of our clients, stakeholders, complaints and employees (including contractors).

In addition, this Policy will provide details for clients, to better understand what information is collected, how the information will be stored and managed by the SBDC and how their personal details will be protected and secured from misuse.

2. Scope

This Policy applies to all persons whether in paid employment, on contract (including contractors and consultants) or undertaking voluntary services for the SBDC (hereinafter referred to as employees).

This Policy applies to information created, collected, and held by the SBDC.

In scope:

- Information collected and or held by the SBDC for the purposes of providing services to clients and stakeholders.
- Information created by the SBDC for the purposes of providing services to clients and stakeholders.
- Information provided by clients and stakeholders, including personal information required for the purpose of providing specific services.
- Information by complainants

Out of scope:

- Aggregated statistical data about our clients, stakeholders, and services, where no personal identifying information is contained, collected, or shared for the purposes of improving the SBDC's services to small businesses within Western Australia.

3. Policy Definitions

Information Privacy	Establishment of rules governing the collection and handling of personal data. <i>(as defined by the Australian Law Reform Commission)</i>
	Information privacy is about promoting the protection of information that says who we are, what we do and what we believe. <i>(Office of the Australian Information Commissioner)</i>
	Is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, contextual information norms, and the legal and political issues surrounding them. (also known as Data Privacy or Data Protection) <i>(Wikipedia)</i>
Privacy	Is the fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination.
	Is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively. <i>(Wikipedia)</i>
Sensitive Information	Sensitive information is defined in the <i>Privacy Act 1988</i> to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information. Sensitive information will be used by us only: • for the primary purpose for which it was obtained • for a secondary purpose that is directly related to the primary purpose • with your consent; or where required or authorised by law.

Confidentiality	Defined in common law, refers to information that is not in the public domain and the process of using one's discretion or an obligation or right to withhold certain information, transactions from others, particularly to external parties. Confidentiality is covered by legislative requirements, more specifically the <i>Small Business Development Corporation Act 1983 S18 & S18AA</i>. Release of confidential personal information must only be with written consent from the person to whom the information relates to, for example, discussing case information within the team of the SBDC is not a breach of confidentiality. Where the information relates to a complainant the confidentiality of the information can also be kept or maintained secret at the discretion of the Commissioner.
------------------------	--

4. Policy Statement

The intent of this Policy is to enable the SBDC to outline and commit to its corporate responsibilities around the proper collection, management, use and disclosure of information about its clients, stakeholders and employees in accordance with industry standards and legislation; and use the information provided to:

- continue to build a strong and enterprising small business sector in Western Australia,
- deliver and facilitate relevant, practical support to small businesses, and
- advocate on the behalf of small businesses with strong supporting evidence.

5. Disclosure of Personal Information

Your Personal Information may be disclosed in a number of circumstances including the following:

- Third parties where you consent to the use or disclosure; and
- Where required or authorised by law.

6. Information provided by third parties

Where reasonable and practicable to do so, we will collect your Personal Information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

7. Updates and access

This Policy, its principles and guidelines will be reviewed regularly and updated as required.

Access to your Personal Information

You may access the Personal Information we hold about you to read, update and/or correct it, subject to certain exceptions. If you wish to access your Personal Information, please contact us in writing through the Freedom of Information application form.

The SBDC will not charge any fee for your access request but may charge an administrative fee for providing a copy of your Personal Information.

In order to protect your Personal Information, we may require identification from you before releasing the requested information.

8. Principles

In line with the Australian Privacy Principles, the SBDC commits to the following principles:

1. Open and transparent management of personal information.
 - a. The SBDC commits to complying with relevant legislation and associated principles and guidelines through ensuring the maintenance of a Privacy Policy and making this Policy available to all clients and stakeholders.
2. Anonymity and pseudonymity.
 - a. The SBDC allows individuals not to identify themselves, where reasonably practicable, when seeking services from the Corporation.
 - b. An individual may use a pseudonym when interacting with the SBDC, where SBDC will treat the pseudonym as the correct details as provided.

- c. It is acknowledged that by not providing some personal details, this may limit the amount and specific type of information that can be provided to the individual.
 - d. An individual can only act on behalf of a business and not purport to be the business.
- 3. Collection of solicited personal information.
 - a. The SBDC commits to only collecting relevant personal information that is required for the purpose of providing specific services to them as an individual or on behalf of themselves or their business.
 - b. Individuals accessing the SBDC's services are made aware of the requirements of collecting personal details and how they are used and stored for the purpose of providing that service and its primary and secondary purposes.
- 4. Dealing with unsolicited personal information.
 - a. Personal information provided where not required, will be protected, and be assessed for retention requirements, and either returned to the individual involved, redacted, or deleted from its systems.
- 5. Notification of the collection of personal information.
 - a. The SBDC will notify individuals by appropriate means that personal information may be collected as and when required, to provide a service.
- 6. Use or disclosure of personal information.
 - a. The SBDC will use personal information collected for the primary purpose of providing information and services specific to the individual requesting it.
 - b. The SBDC will use personal information and disclose some personal information relevant for contacting individuals for the secondary purpose of evaluating performance of the SBDC in surveys of clients who have used the SBDC's services.
 - c. The SBDC will disclose personal information when requested and required or authorised by or under an Australian or Western Australian law or a court/tribunal order.
- 7. Direct marketing
 - a. The SBDC will use an individual's email address if provided to market goods and services directly to them.
 - b. Each person can opt-out of these communications at any time of their choosing.

8. Cross-border disclosure of personal information.

- a. The SBDC may from time to time disclose personal information to relevant Government agencies, where agreements are in place or referrals are required and upon agreement with the client themselves to do so.
- b. The SBDC will not disclose your personal details to anyone outside of Australia, unless authorised to do so (for example, to Migration agents, via a Form 956)

9. Quality of personal information.

- a. The SBDC commits to ensuring that personal information provided and collected will be accurate, up-to-date, and complete.

10. Security of personal information.

- a. The SBDC commits to ensuring to take such steps to ensure that personal information provided is protected from misuse, interference and loss or unauthorised access, modification, or disclosure.
- b. If determined that the SBDC no longer requires personal information, the SBDC will ensure that it is appropriately disposed of and destroyed under appropriate disposal authorities approved by the State Records Office, unless otherwise by law required to retain the information.

11. Access to personal information.

- a. An individual whose personal information is held and maintained by the SBDC for the purpose of providing services, can on request, access their personal information. This request must be done a Freedom of Information application.

12. Correction of personal information.

- a. If personal information held by the SBDC is incorrect, the individual may request and have the SBDC update their information to represent their personal details correctly.

9. Guidelines

1. Individuals providing information to the SBDC have the right to have their privacy respected.
2. In some instances, individuals can decide that they do not wish to provide any personal details to identify them, however, this may impact the quality and specificity of the response and service provided.
3. Personal information collected is specific for its needs, assessment, and provision of service at the time of collection.
4. Personal information provided is considered correct and accurate at the time of receipt until otherwise corrected.
5. Personal information collected must be confirmed for its accuracy and completeness for entry into any SBDC systems.
6. Personal information collected that is reported as being incorrect, will be updated at the request of the person to whom the details relate.
7. A third party cannot request an update to personal data unless authorisation has been given and received.
8. Personal information collected will be stored appropriately, in the correct systems in accordance with the SBDC's approved Information Management Policies.
9. Personal information collected, stored, and maintained by the SBDC will be classified appropriately within the systems it is stored and access prevented by those who are not authorised or do not have a business need to access the details.
10. Personal information will not be provided to any third parties for monetary gain or profit.



10. Personal information we collect and hold

General Information	Marketing and Communications	Disputes and Investigations	Grants	Business migration	Employee and contractor
• First name • Last name • Phone number • Mobile number • Email address • Business duration • Postcode or suburb	• General Information + • Business industry • Services used • Service surveys and responses • Testimonials and feedback either provided directly or through third party platforms (i.e. google) •	• General Information + • Business name • Position in business • Third parties related to the dispute or investigation (including specific individuals associated with that third party where it is a business. • Contracts associated with the dispute or investigation.	• General Information + • Business name • Position in business • Related contacts (Director or accountant) • *Driver's licence • Bank account details and statements • Business registration information (ABN, Address, trading names) • Social media	• General Information + • Date of Birth (Age) • Gender • Biometrics (photos) • Passport details • Country of Birth • Country of Residence • Current visa details • Education • Relationships (Partners, Dependants, subject to the application) • Bank Statements	• General Information + • Personal address • Emergency contact/ next of kin details • Salary and leave records. • Superannuation • Taxation • Bank account details • Medical certificates and other health related information • Training certificates • Performance and conduct information. • Education

General Information	Marketing and Communications	Disputes and Investigations	Grants	Business migration	Employee and contractor
			Payroll details of employees (excluding TFNs).	- Personal financial status and assets (including abroad and locally) - Business financials and assets (including abroad and locally) - Payroll details of employees (excluding TFNs) - Business registration information. - Personal Address - Criminal and financial declarations	- Job applications - Conflicts of interest
Collected over the phone or via online forms for the purpose of returning contact for advice.	Collected over phone or via online forms in response to an opt in for marketing		Driver's licence may not always be sought but is requested from time to time as a form of verification.		

General Information	Marketing and Communications	Disputes and Investigations	Grants	Business migration	Employee and contractor
Includes workshop participants.	- Collected via third party sources for example other Government authorities and contracted parties. - Collected via workshops.				
Information collected for this purpose allows the SBDC to provide specific advice in relation to your enquiry	Information collected for this purpose allows the SBDC to inform you of services that may be of interest to you.		Information collected for this purpose is to verify you, your relationship to the business and your authority to act on behalf of the business for the business to receive funding from the Western Australian government or Grantors through the SBDC systems.	Information collected for this purpose is required for assessing suitability for the program.	Information collected for this purpose is to ensure that the SBDC have sufficient relevant information for your employment within the Western Australian Public Service.

General Information	Marketing and Communications	Disputes and Investigations	Grants	Business migration	Employee and contractor
General enquiries and information are maintained for 2 years.	General enquiries and information are maintained for 2 years.	Information relating to disputes and investigations can be maintained between 7 and 20 years, depending on the severity of the dispute or investigation and its impact to the State.	Grants information is maintained for 6 years after successful audit.	Business migration applications and nominations are maintained between 2 and 7 years, depending on the outcome of assessment or withdrawal status (2 years if declined or withdrawn) or If approved and required to submit the second stage application for permanent residency sponsorship for business is 7 years after application approval.	Employee records are transferred to any receiving state government agency or maintained for 70 years after birth or 6 years after retirement or cessation of employment, whichever is later.

11. How we secure personal information

The SBDC will take reasonable steps to ensure that personal information we collect is held securely. This includes protecting personal information from:

- Loss
- Unauthorised access
- Misuse
- Modification
- Unlawful disclosure.

Personal information that we hold is managed securely through our record-keeping systems. We ensure we safeguard our ICT systems against unauthorised access and ensure that paper-based files are physically secured. We ensure that personal information within our systems is only accessible to staff on a need-to-know basis. These systems are regularly reviewed and tested to ensure protection.

12. Roles and Responsibilities

Employees

All employees are responsible for:

- Understanding and complying with this policy while in the workplace or representing the SBDC.
- Advising clients and stakeholders of the appropriate methods of obtaining or correcting their personal information.
- Advising management if they believe the policy may have been breached in line with the Data Breach Policy and Data Breach Procedure.

Managers and Senior Leadership Team

Managers are responsible for:

- Supporting and contributing to the implementation of this policy.
- Providing new employees with an understanding of this policy during their induction to SBDC.
- Ensuring team business and events are conducted in line with this policy and promoting an awareness of this policy amongst employees.

- Assisting in the review of the policy and systems to ensure that appropriate measures are in place to as best as possible inform and enforce with staff the requirements of this policy prevent breaches.

Executive Leadership Team

The Executive Leadership Team is responsible for:

- Implementing and enforcing this policy, its objectives and purpose.
- Ensuring the Senior Leadership Team and all employees understand their obligations and responsibilities under this policy and the individual right to privacy and data protection.
- Ensuring a review is undertaken in the event of a privacy breach and acting to ensure that measures are taken to prevent future breaches in consultation with the Data Breach Policy and Data Breach Reporting Procedure.

Board

The Board is responsible for:

- Ensuring that members are aware of and understand the Policy as it relates to them, their role and the information provided to them in that role.

Information Technology

The Information Technology team is responsible for:

- Ensuring that systems are maintained, and patching and security software and measures are in place to appropriately secure private data.
- Ensuring where alerts are received on private data being transferred inappropriately or unusually out of systems, notifications are sent to the appropriate directors or managers where a breach may be suspected.

RACI Table

Defined roles outlined in the Information Asset Register, the Information Management Governance Framework and the Information Management key definitions and roles and responsibilities.

	Identify	Correctness	Update	Protect/secure	Review	Dispose
Employees	A	R	R	C	C	I
Information Sponsors and Stewards	A	A	A	A	A	C
Information Owner	R	I	I	C	C	C
Manager Information Governance	C	C	I	R	R	A
Information Technology	C	I	I	A	R	C
Board	I	I	I	C	I	I
Minister	I	I	I	I	I	I

13. Relevant Legislation

- *Privacy and Responsible Information Sharing Act 2024 (WA)*
- *Freedom of Information Act 1992 (WA)*
- *Privacy Act 1988 (Cth)*

14. Related Policies and Procedures

- Information Access, Use and Disclosure Policy
- Data Breach Policy and Procedure

15. Relevant forms

- [Freedom of Information application form](#)
- Data Breach report