

Policy number	59	Version	1.3
Drafted by	Administration	Approved by CEO on	16.06.2026
Responsible person	CEO	Scheduled review date	16.06.2029
		Category	Governance

INTRODUCTION

Swan City Youth Service Inc. (SCYS) understands the importance of keeping your personal information safe and respecting your right to privacy. We only collect the information we need to provide our services and meet legal requirements. This policy explains how we collect, use, store, and protect your personal information.

SCYS also uses secure digital systems and approved technologies to support service delivery, communications, administration and operational functions.

PURPOSE

This Privacy Policy explains what information we collect from you, how we collect it, and how we use it. SCYS follows the Australian Privacy Principles to ensure your personal information is handled safely and responsibly.

SCYS maintains additional governance procedures relating to digital communications, cybersecurity, data governance and approved AI-assisted technologies.

We are committed to protecting your privacy and only collect personal information, when necessary, to provide services, meet legal requirements, or comply with funding and reporting obligations.

SCYS is committed to managing information in a manner that supports privacy, responsible information sharing, safeguarding obligations and evolving legislative requirements.

SCYS recognises that privacy, information governance, cybersecurity and safeguarding are interconnected responsibilities that contribute to the safety, wellbeing and rights of young people.

RELEVANT LEGISLATION

- Privacy Act 1988 (Cth)
- Privacy and Responsible Information Sharing Act 2024 (WA)
- Australian Privacy Principles, Spam Act 2003
- Online Safety Act 2021
- Notifiable Data Breaches Scheme

APPLICATION OF POLICY

This Privacy Policy applies to all individuals and entities engaged by or representing SCYS, including Management Committee members, employees, volunteers, students, contractors, consultants and

approved third-party providers who may access or handle organisational information. Each group has specific responsibilities to ensure personal information is handled securely and in compliance with the Privacy Act 1988 (Cth).

Approved organisational systems, databases, digital platforms, communication tools and third-party providers used by SCYS are also subject to privacy, information governance and cybersecurity requirements.

MANAGEMENT COMMITTEE MEMBERS

The Management Committee maintains governance oversight of privacy, information governance and organisational risk through reporting and assurance processes.

CEO

The CEO is responsible for operational management of privacy matters, complaints and breaches.

- Ensure SCYS has strong privacy policies and procedures in place.
- Oversee compliance with privacy laws and reporting obligations.
- Respect the privacy and confidentiality of all clients, staff, and SCYS operations.
- Review and address any privacy-related complaints or breaches.
- Maintain confidentiality regarding SCYS operations and client information.
- Maintain oversight of cybersecurity, governance and digital risk management.

STAFF MEMBERS

- Collect, store, and use personal information only for lawful and necessary purposes.
- Follow SCYS policies when handling sensitive or confidential information.
- Secure personal data to prevent unauthorised access, misuse, or loss.
- Staff must not enter confidential or identifying information into unauthorised AI or third-party systems.
- Ensure safe use of digital systems.
- Report cyber incidents.
- Report any privacy concerns, breaches, or risks to management immediately.
- Participate in privacy training and comply with data protection guidelines.

VOLUNTEERS

- Volunteers must maintain confidentiality, protect organisational and client information, and comply with SCYS social media, privacy and digital communication requirements at all times.
- Only access personal information necessary for their role.
- Follow SCYS privacy procedures and report any breaches or concerns.
- Seek guidance from staff if unsure about handling private information.

All individuals must comply with this policy. Breaches may result in disciplinary action, removal from SCYS, or legal consequences where required by law.

POLICY

SCYS only collects personal information that is necessary for or directly related to our services, business functions, and activities. This information is always obtained lawfully and fairly, and we will collect it directly from you whenever reasonable and practicable.

SCYS seeks to collect the minimum amount of personal information necessary to provide services, meet legal obligations, support safeguarding responsibilities and fulfil organisational functions.

In some cases, SCYS may collect personal information for funding, reporting, and compliance purposes. This may include national police clearances, Working with Children Checks, and other relevant documentation as required by law.

SCYS handles all personal information in accordance with the Privacy Act 1988 (Cth). Information collected for service delivery, safeguarding, reporting, compliance or operational purposes may be shared where necessary, lawful, proportionate and consistent with privacy, safeguarding and organisational obligations. SCYS takes reasonable steps to ensure personal information is used responsibly, securely stored, and only disclosed where necessary for legal, funding, service delivery or operational purposes.

SCYS takes reasonable steps to ensure third-party providers handling personal information comply with applicable privacy obligations, including where information may be securely processed or stored using cloud-based systems.

SCYS does not collect sensitive information—such as political opinions or associations, membership of professional or trade associations or unions, religious or philosophical beliefs, criminal records, health information, or sexual orientation—without your consent unless required by Australian law or necessary to provide our services.

WHAT INFORMATION WE COLLECT

SCYS may collect personal information including:

- Name, date of birth, and contact details.
- Emergency contact and guardian information where relevant.
- Information required for participation in services, programs, or events.
- Employment, volunteer, student placement, or contractor information where applicable.
- Donation, payment, or transaction information.
- Information provided through enquiries, registrations, forms, communications, or feedback.
- Photographs or videos, where consent has been given.
- Information required for legal, safeguarding, funding, or reporting obligations.
- Website, email, or digital communication information where individuals engage with SCYS through electronic services or communications.
- Unique client identifiers, service participation records, case notes, referrals and other information necessary to support service delivery, safeguarding and organisational reporting.

Where appropriate, SCYS may collect information relating to wellbeing, support needs, or safeguarding requirements necessary to provide safe services.

WHY WE COLLECT YOUR INFORMATION

SCYS collects personal information to:

- Provide, manage, and improve our services, programs, and activities.
- Support the safety, wellbeing and safeguarding of young people, families, staff, and volunteers.
- Communicate with clients, families, donors, supporters, and community members.
- Process donations, payments and provide receipts or other relevant documentation.
- Manage employment, volunteer, contractor, and placement arrangements where applicable.
- Meet legal, funding, reporting, and contractual obligations.
- Maintain organisational records and operational systems.
- Respond to enquiries, feedback, incidents, or complaints.
- Support approved marketing, community engagement, and promotional activities where consent has been provided.
- Protect the security and integrity of SCYS systems, services, and information.
- Conduct service planning, evaluation, and quality improvement activities.

If you choose not to provide certain details, we may not be able to offer full access to our services.

HOW WE MANAGE AND SHARE YOUR INFORMATION

SCYS manages personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles and other applicable legislation.

Personal information is only accessed by authorised staff, volunteers, contractors or approved third-party service providers where necessary to support service delivery, operational functions, legal obligations, safeguarding responsibilities or funding and reporting requirements.

SCYS takes reasonable steps to ensure personal information is:

- used lawfully and responsibly,
- securely stored and protected,
- only disclosed where necessary or permitted by law,
- and retained and disposed of in accordance with legal, contractual, and operational requirements.

SCYS may use approved digital, cloud-based and third-party systems, including the SCYS Database, to support service delivery, administration, communications, donations, reporting, safeguarding and organisational operations. Reasonable steps are taken to ensure these systems appropriately protect personal information and comply with relevant privacy obligations.

SCYS will take reasonable steps to consider privacy, safeguarding and information security requirements when implementing new technologies, systems or digital services.

Privacy considerations may include access controls, data retention requirements, information classification, cybersecurity risks, safeguarding requirements and the potential impact on young people and other individuals.

SCYS maintains reasonable cybersecurity and information security practices designed to support the safe handling and protection of personal information.

Where consent has been provided, photographs and videos may be used in promotional material in accordance with SCYS policies and procedures. SCYS will not knowingly publish identifying information that may place a young person or individual at risk.

Personal information will only be retained for as long as required by law, funding obligations, operational requirements, safeguarding responsibilities or service delivery purposes.

SCYS maintains record retention and disposal requirements through its Record Management and Information Governance framework.

When information is no longer required, records will be securely destroyed, de-identified or deleted using approved organisational processes appropriate to the storage medium and system involved.

INFORMATION GOVERNANCE

SCYS maintains information governance practices to support the lawful, ethical and secure management of organisational information.

Information governance activities may include:

- information classification;
- access management;
- record retention and disposal;
- cybersecurity controls;
- approved technology use;
- data quality and accuracy;
- privacy and safeguarding considerations;
- incident and breach management.

Information governance responsibilities apply to all staff, volunteers, students, contractors and authorised users of SCYS systems.

YOUR RIGHTS AND CHOICES

You may request access to the personal information SCYS holds about you and request corrections where information is inaccurate, incomplete, or out of date.

Where consent has been provided previously, you may withdraw your consent at any time by contacting SCYS in writing. SCYS will take reasonable steps to stop future use of your information, photographs, or video recordings where practicable, however information already published or shared externally may not be fully removable.

You may choose to opt out of receiving marketing or promotional communications from SCYS at any time.

SCYS may require verification of identity before releasing or updating personal information.

If you have concerns about how your personal information has been managed, you may contact SCYS to make a privacy enquiry or complaint. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC).

SCYS will take reasonable steps to respond to privacy requests and complaints within an appropriate timeframe.

CHILD SAFETY AND SAFEGUARDING

SCYS is committed to protecting the safety, wellbeing, dignity and privacy of children, young people and vulnerable individuals accessing our services.

Privacy obligations will be balanced with child safety, safeguarding, mandatory reporting and legal obligations where concerns exist regarding the safety or wellbeing of a young person.

SCYS takes reasonable steps to ensure personal information relating to children and young people is collected, used, stored, and shared in a manner that supports child safety, safeguarding obligations and privacy requirements.

Photographs, videos and identifying information relating to young people will only be used where appropriate consent has been obtained and where the use does not place the young person at risk.

SCYS will not knowingly publish or disclose information that may compromise the safety, wellbeing or confidentiality of a child or vulnerable person.

All staff, volunteers, contractors, and representatives of SCYS are expected to maintain appropriate professional boundaries, protect confidential information and comply with SCYS safeguarding, privacy and digital communication requirements at all times.

SECURITY AND DATA BREACHES

SCYS takes reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure through appropriate administrative, physical and digital security measures.

SCYS maintains cybersecurity and information security practices designed to support the safe handling and protection of personal information, including secure systems, restricted access controls, and staff awareness practices.

If SCYS becomes aware of a privacy breach, data breach or cybersecurity incident, reasonable steps will be taken to assess the incident, mitigate risks and meet any applicable reporting, notification and legal obligations. Where required by law, affected individuals, regulators, funding bodies or other relevant authorities will be notified.

SCYS maintains processes for reporting, investigating, managing and reviewing privacy breaches, cybersecurity incidents and unauthorised disclosures of information as part of its continuous improvement and risk management activities.

PRIVACY COMPLAINTS OR QUESTIONS

If you have any concerns or want to correct your personal information, contact us.

Email: reception@scys.org.au

Mail: Swan City Youth Service Inc., 12 Padbury Terrace, Midland WA 6056

If you are not satisfied with our response, you can contact the Office of the Australian Information Commissioner at www.oaic.gov.au.

CHANGES TO THIS POLICY

SCYS may update this Privacy Policy from time to time to ensure it remains consistent with changes to legislation, regulatory requirements, technology, service delivery practices and emerging privacy, cybersecurity, and digital communication risks.

Any updates will be published through appropriate SCYS communication channels, including the SCYS website where applicable.

CONSEQUENCES OF BREACH OF THIS POLICY

All employees, volunteers, contractors, Management Committee members, students and authorised representatives of SCYS are required to comply with this Privacy Policy and associated governance procedures.

Any breach of this policy, including misuse of personal information, unauthorised disclosure, inappropriate use of digital systems, cybersecurity breaches or misuse of social media or communication platforms, may result in appropriate action being taken by SCYS.

Depending on the nature and severity of the breach, actions may include:

- investigation of the incident,
- additional training or corrective action,
- restriction or removal of system access,
- disciplinary action,
- termination of employment, engagement or volunteer involvement,
- and reporting to relevant authorities where required by law.

SCYS will manage privacy and data breaches in accordance with applicable legislation, organisational procedures and reporting obligations, including notification requirements under the Notifiable Data Breaches Scheme where applicable.

Authorisation



Signature of CEO, Swan City Youth Service