



SECC

Privacy and Confidentiality Policy

Purpose

This policy explains how South Eastern Community Connect (SECC) manages personal information, including sensitive and health information. It covers how SECC collects, holds, uses, discloses, secures, provides access to, corrects, retains and disposes of information, and how SECC responds to privacy complaints and actual or suspected privacy breaches.

SECC is committed to respecting each person's dignity, autonomy, privacy and confidentiality and to managing personal information lawfully, fairly, transparently and in a way that supports safe, high-quality services.

Scope

This policy applies to all SECC programs, services, locations, systems and records, and to all people who handle personal information for or on behalf of SECC, including Board members, employees, volunteers, students, contractors, consultants, labour-hire workers, service providers and suppliers.

It applies to personal information in any form, including paper records, electronic records, databases, emails, photographs, video and audio recordings, CCTV footage, telephone notes, cloud-hosted information and information created or received through mobile or remote work.

Where another law, funding agreement, professional obligation or service-specific policy imposes a higher standard, the higher standard applies. This policy should be read with the Privacy and Confidentiality Procedure and approved records-retention schedule.

Definitions

Term	Definition
APPs	The Australian Privacy Principles in Schedule 1 to the Privacy Act 1988 (Cth).
Authorised representative	A person lawfully authorised to act for an individual, such as a guardian, attorney, registered supporter or other representative recognised under applicable law. Authority must be verified and recorded.
Confidential information	Information that is not publicly available and that SECC has an obligation to protect, including personal information, client records, employee information, commercial information and information received in confidence.
Consent	Voluntary, informed, current and specific agreement by an individual with capacity, or by an appropriately authorised representative. Consent may be express or implied where the law permits, but express consent is preferred for sensitive information, media and non-routine disclosure.
Data breach	Unauthorised access to, unauthorised disclosure of, or loss of personal information, including a suspected breach.

Term	Definition
Eligible data breach	A data breach that meets the notification threshold under Part IIIC of the Privacy Act 1988 (Cth), including where unauthorised access, disclosure or loss is likely to result in serious harm and remedial action has not prevented that likelihood.
Health information	Personal information or an opinion about a person's physical or mental health or disability; a health service provided or to be provided; a person's expressed wishes about future health services; personal information collected in providing a health service; certain donation information; or genetic information that is or could be predictive of health.
HPPs	The Health Privacy Principles in the Health Records and Information Privacy Act 2002 (NSW).
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information is true and whether or not it is recorded in material form.
Privacy Officer	The Privacy Officer is the person designated by SECC to oversee privacy governance, enquiries, complaints, breach response, training and review. At SECC, this function rests with the Chief Executive Officer.
Sensitive information	Personal information about racial or ethnic origin; political opinions or associations; religious or philosophical beliefs or affiliations; membership of a professional or trade association or trade union; sexual orientation or practices; criminal record; health information; genetic information not otherwise health information; biometric information used for automated biometric verification or identification; or biometric templates.
Worker	Any Board member, employee, volunteer, student, contractor, consultant, labour-hire worker or other person performing work for or on behalf of SECC.

Policy Statements

1. Privacy principles and accountability

- SECC manages personal information openly and transparently and maintains governance arrangements proportionate to the nature, volume and sensitivity of the information it holds.
- SECC collects only information reasonably necessary for its functions or activities and, for sensitive information, obtains consent unless collection is otherwise required or authorised by law.
- Personal information is only accessed by people who need it to perform authorised duties. Curiosity, convenience or seniority does not create a right of access.
- All workers must protect confidentiality during and after their engagement with SECC and must complete required privacy, records management and cyber security training.
- SECC's CEO will take on the role of Privacy Officer and maintain documented privacy responsibilities, breach escalation pathways, registers and review arrangements.

2. Anonymity and pseudonymity

SECC will provide individuals with the option of dealing anonymously or by pseudonym where this is lawful and practicable. SECC may require identity information where it is required or authorised by law, necessary to deliver a service safely, needed to verify authority, or otherwise impracticable to provide the service without identifying the person.

3. Collection of personal information

- SECC collects personal information by lawful and fair means and, where reasonable and practicable, directly from the individual.
- Information may be collected from an authorised representative, family member, carer, supporter, health professional, government agency, service provider, referee or other third party where the individual consents or collection is otherwise permitted by law.
- SECC will take reasonable steps to ensure information collected is relevant, accurate, up to date, complete and not excessive for the purpose.

- Audio, photographs, video, voice recordings and promotional material that identify a person will only be created or used with appropriate consent or another clear lawful authority. Consent for service delivery must not be bundled with optional promotional consent.
- Consent to use a person's image, voice or story will record the channels, purposes and time period it covers. Reuse for a materially different purpose, such as a story collected for a newsletter and later used in a fundraising appeal, requires fresh consent. Consent may be withdrawn at any time. SECC will stop future use, though material already printed, published or shared by others cannot be recalled, and this will be explained at the time consent is given. Contractors engaged to photograph, film, write or design will not use, retain or publish SECC material, including raw files, for their own purposes.
- Where SECC receives unsolicited personal information, it will determine whether the information could lawfully have been collected. If not, SECC will, where lawful and reasonable, securely destroy or de-identify it.

4. Collection notices and transparency

At or before collection, or as soon as practicable afterwards, SECC will take reasonable steps to provide a clear privacy collection notice. The notice will be communicated in a language, format and mode the individual is likely to understand and will address, as applicable:

- SECC's identity and contact details;
- the facts and circumstances of collection, including collection from another person;
- why the information is being collected and how it will be used;
- whether collection is required or authorised by law and the relevant authority;
- the main consequences if the information is not provided;
- the usual types of recipients to whom the information may be disclosed;
- how to access or correct personal information and how to make a complaint;
- whether SECC is likely to disclose information to overseas recipients and, where practicable, the countries involved; and
- any additional notice required by the NSW Health Privacy Principles or service-specific legislation.

5. Capacity, consent and representatives

- SECC will presume an adult has decision-making capacity unless there is a lawful and reasonable basis to conclude otherwise.
- Information and choices will be explained in an accessible way, with communication support, interpreters, advocates or supporters offered where appropriate.
- Before relying on a representative, SECC will verify identity, authority and the scope and currency of that authority.
- Children and young people will be involved in privacy decisions to the extent appropriate to their age, maturity, capacity, wishes and applicable law. Family relationship alone does not establish authority to access or disclose a child's information.
- Consent may be withdrawn prospectively, subject to lawful, safety, contractual and recordkeeping requirements. Withdrawal and its consequences will be documented.

6. Use and disclosure

SECC will use or disclose personal information for the primary purpose for which it was collected. Use or disclosure for another purpose will occur only where:

- the individual has consented;
- the secondary purpose is related to the primary purpose, or directly related for sensitive information, and the individual would reasonably expect the use or disclosure;
- the use or disclosure is required or authorised by an Australian law or court or tribunal order;
- a permitted general situation or permitted health situation applies; or
- another specific legal authority applies.

Possible disclosures may include authorised service providers, health professionals, funding bodies, auditors, insurers, legal advisers, regulators, emergency services or government agencies where the disclosure is lawful and necessary. SECC will disclose only the minimum information reasonably necessary and will record material non-routine disclosures.

A suspicion that a crime has occurred, a concern about self-harm, or a belief that another person may be at risk does not automatically authorise disclosure. Workers must promptly escalate the matter under the relevant safety, incident, safeguarding or mandatory-reporting procedure so that the lawful basis, urgency and minimum necessary disclosure can be assessed.

7. Children's information

SECC will handle children's personal information in accordance with applicable education and care, child-protection, information-sharing, mandatory-reporting and privacy laws. Information may be disclosed to a parent, guardian or other authorised person only after authority and any relevant safety restrictions have been checked. Information may also be disclosed to a regulator, child-protection body, police or another person or body where required or authorised by law. The child's safety, participation rights and best interests will be considered in accordance with applicable law.

8. Direct marketing, fundraising and communications

- SECC will only use personal information for direct marketing or fundraising where permitted by law and consistent with reasonable expectations or valid consent.
- Communications will identify SECC and provide a simple means to opt out where required. Opt-out requests will be actioned promptly and recorded.
- Sensitive information will not be used for direct marketing without consent unless expressly permitted by law.
- Contact lists will not be sold or disclosed to another organisation for its own marketing unless the individual has clearly consented and the disclosure is lawful.
- SECC's website, email platforms and social media accounts may collect personal information through analytics, cookies, tracking tags, email open and click tracking, and account interactions. SECC will explain this in its website privacy statement and will assess each tool under section 10 before it is installed.
- SECC will not upload contact lists to an advertising platform for audience matching or targeting unless the disclosure is lawful, disclosed to individuals and approved by the Privacy Officer. Client contact details will not be used for this purpose.
- Comments, direct messages, reviews and tagged content may contain personal, sensitive or health information. Workers will not respond publicly with any personal detail, will escalate complaints and safety concerns under sections 13 and 17 and the Feedback and Complaints Management Policy, and will hide or remove content that identifies a person's involvement with a service.
- Journalists, photographers, funders, politicians and other visitors will not be given access to clients, premises or records without CEO approval. Client information will not be disclosed to media at any time. Any client taking part must give separate consent.

9. Government-related identifiers

SECC will not adopt a government-related identifier as its own identifier, or use or disclose such an identifier, unless the action is required or authorised by law or otherwise permitted under the APPs. Examples include Medicare numbers, Centrelink reference numbers and government-issued client identifiers.

10. Third-party, cloud and overseas handling

- Website, analytics, advertising, email marketing and design platforms are service providers for the purposes of this section. Many store or process information overseas. Before engaging a service provider that will handle personal information, SECC will assess privacy, security, location, access, subcontracting, retention, breach-notification and return or deletion arrangements.

- Contracts will include confidentiality, authorised-use, security, incident reporting, cooperation, audit or assurance, data-return and secure-disposal requirements appropriate to the risk.
- Before disclosing personal information overseas, SECC will take steps required by APP 8 and document the basis for the disclosure. Individuals will be informed of likely overseas disclosures through the privacy policy or collection notice where required.
- Workers must not store or transmit SECC personal information using unapproved applications, personal email accounts, removable media or consumer cloud services.

11. Information quality

SECC will take reasonable steps to ensure personal information is accurate, up to date, complete and relevant, having regard to the purpose for which it is used or disclosed. Workers must distinguish fact from opinion, record information objectively, identify the source where relevant, and correct known errors promptly.

12. Security and confidentiality

SECC will take reasonable technical, physical and organisational steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Controls will be proportionate to the sensitivity of the information and may include:

- role-based access and least-privilege permissions;
- individual user accounts, strong authentication and multifactor authentication where available;
- approved password-management arrangements; passwords must not be kept in readable shared registers;
- encryption and secure transfer methods for sensitive information;
- locked storage, clear-desk practices and secure printing, transport and disposal of paper records;
- device management, screen locking, patching, backups, malware protection and remote-access controls;
- logging, monitoring and periodic access reviews;
- prompt removal or adjustment of access when roles change or engagement ends;
- privacy and security assessments for new systems, services and material changes; and
- confidentiality and security controls for third parties.

13. Privacy breaches and the Notifiable Data Breaches scheme

All actual or suspected privacy breaches, lost devices, misdirected communications, unauthorised access and near misses must be reported immediately through SECC's incident and privacy-breach process. Workers must not investigate independently, conceal the incident, contact affected people without authorisation, or delete relevant evidence.

SECC will promptly contain the incident, preserve evidence, assess the information and people affected, evaluate the risk of serious harm, take remedial action, document decisions and notify insurers, regulators, funding bodies, partners or affected individuals where required.

Where there are reasonable grounds to suspect an eligible data breach under the Privacy Act, SECC will complete the legally required assessment within the applicable statutory period. If an eligible data breach has occurred and no exception applies, SECC will prepare the required statement for the Australian Information Commissioner and notify affected individuals in the manner required by law. SECC will also assess other notification duties, including contractual, aged-care, health, child-safety and cyber-security obligations.

14. Access to personal information

- Individuals may request access to personal information SECC holds about them. Requests should be directed to the Privacy Officer or the relevant service, and reasonable assistance will be provided.
- SECC will verify identity and, for a representative, authority before granting access.
- Requests will be handled within the time required by applicable law. Where no specific shorter period applies, SECC will respond within a reasonable period.

- Access will be provided in the requested form where reasonable and practicable. A charge will not be imposed for making a request; any permitted access charge will be reasonable and advised in advance.
- Access may be refused or limited only on a lawful ground. Where practicable, SECC will consider redaction, supervised inspection, an intermediary or another form of access.
- If access is refused, SECC will provide written reasons and available complaint mechanisms unless doing so would be unlawful or unreasonable.

15. Correction of personal information

- Individuals may ask SECC to correct information they believe is inaccurate, out of date, incomplete, irrelevant or misleading.
- SECC will take reasonable steps to correct information where satisfied a correction is required, having regard to the purpose for which the information is held.
- If SECC refuses a correction request, it will provide written reasons and complaint options unless doing so would be unlawful or unreasonable and will take reasonable steps to associate a statement of the requested correction with the record.
- Where appropriate and lawful, SECC will notify relevant third parties to whom incorrect information was previously disclosed.

16. Retention, de-identification and disposal

- Personal information will be retained only for as long as required for service delivery, legal and regulatory obligations, funding and contractual requirements, safeguarding, insurance, complaints, investigations, potential claims, business continuity and approved archival purposes.
- Retention and disposal will follow SECC's approved records-retention schedule. A single seven-year rule must not be applied to all records without considering the record type and applicable requirements. Consent records for published images, voice recordings or stories must be retained for as long as the asset remains in circulation and for any further period required by the approved records-retention schedule. Opt-out records must be retained for as long as needed to demonstrate and honour the opt-out.
- Destruction, deletion or de-identification will be suspended where a complaint, investigation, audit, subpoena, legal hold, claim or anticipated proceeding applies.
- When information is no longer required and SECC is legally permitted to dispose of it, it will be securely destroyed or de-identified. Disposal must include copies held in approved systems and by service providers where practicable and required.
- De-identified information will be managed to minimise the risk of re-identification.

17. Privacy complaints and enquiries

Privacy enquiries and complaints may be made verbally or in writing, directly or through an authorised representative, and with communication support where needed. They should be directed to the Privacy Officer or managed under SECC's Feedback and Complaints Management Policy.

- SECC will acknowledge, assess and respond to complaints fairly, promptly, confidentially and without reprisal.
- The person will be told the outcome, reasons and available internal or external review options.
- Complaints will be recorded, investigated by a person with appropriate authority and managed for conflicts of interest.
- Individuals may also have a right to complain to the Office of the Australian Information Commissioner, the NSW Privacy Commissioner, the Aged Care Quality and Safety Commission or another relevant regulator. SECC will provide regulator details appropriate to the matter.
- Complaint information will be analysed for systemic issues and continuous improvement.

18. Aged care privacy and protected information

- SECC will deliver funded aged care services in a way that respects personal privacy, dignity, choice, autonomy and the Statement of Rights.

- Older people will be supported to control who receives their information and how supporters, representatives, families and carers are involved, subject to capacity, authority, safety and legal obligations.
- Privacy will be respected during personal care, assessments, home visits, conversations, telehealth, transport and service coordination.
- Protected information under aged-care legislation will only be used, recorded or disclosed where authorised.
- Privacy practices will align with the Aged Care Code of Conduct, applicable Aged Care Quality Standards, incident management and provider-governance obligations.

19. Responsibilities

Role	Responsibilities
Board	Approves the policy; oversees material privacy, information-security and compliance risk; and receives assurance and material incident reporting appropriate to its governance role.
Chief Executive Officer	Ensures this policy is implemented; assigns accountable officers; approves material breach decisions and regulatory notifications as required; and provides governance assurance to the Board.
Privacy Officer	Maintains the privacy framework; provides advice; coordinates access, correction, complaints and breach response; maintains registers; monitors legal change; and arranges training and review.
Senior managers and managers	Implement controls in their areas; restrict access; ensure collection notices and consent practices are followed; manage service providers; report incidents; and monitor compliance.
All workers	Access information only for authorised work; follow privacy and security procedures; verify recipients; maintain accurate records; complete training; and immediately report breaches, risks and concerns.
Service providers and suppliers	Comply with contract, confidentiality, privacy, security, retention and incident-reporting obligations and return or securely dispose of information as directed and required by law.

20. Training, monitoring and review

- Privacy and confidentiality requirements will form part of induction and refresher training, with additional role-specific training for workers who handle sensitive or high-risk information.
- SECC will monitor compliance through incident and complaint trends, access reviews, audits, service-provider assurance, training records, privacy impact assessments and policy review.
- A privacy impact assessment will be considered for new or materially changed projects, technologies, data uses, surveillance arrangements, information-sharing initiatives and artificial intelligence applications involving personal information.
- This policy will be reviewed after a material breach, significant legal or operational change, regulator finding or identified control weakness, and otherwise in accordance with the scheduled review date.

Related Documents

- ORG 7.1: Privacy and Confidentiality Procedure
- ORG 7.1.1: Managing Your Information – Client Information
- ORG 7.1.2: Consent to Use Client Image or Voice in Promotional Materials Form
- ORG 7.1.3: Consent to Release Information Form
- PP4: Feedback and Complaints Management Policy
- PP5: Information Management and Privacy
- SECC Aged Care Policy Handbook
- Data Breach Response Plan and Privacy Breach Register
- Records Management Policy and approved Records Retention and Disposal Schedule
- Information Security / Cyber Security Policy and Acceptable Use requirements
- Incident Management, Child Safe, Mandatory Reporting and Safeguarding policies
- Business Continuity and Disaster Recovery arrangements
- Contractor, procurement and third-party risk management requirements

Regulatory Environment

The following instruments and standards are relevant according to the services SECC provides. The Privacy Officer must maintain this list and confirm applicability when the policy is reviewed:

- Privacy Act 1988 (Cth), including the Australian Privacy Principles and Part IIIC (Notifiable Data Breaches scheme)
- Health Records and Information Privacy Act 2002 (NSW), including the Health Privacy Principles
- Aged Care Act 2024 (Cth), current Aged Care Rules, Statement of Rights, Aged Care Code of Conduct and applicable Aged Care Quality Standards
- My Health Records Act 2012 (Cth), if SECC accesses or uses the My Health Record system
- Education and Care Services National Law and Education and Care Services National Regulations, where applicable
- Children and Young Persons (Care and Protection) Act 1998 (NSW) and other applicable child-protection, information-sharing and mandatory-reporting requirements
- Spam Act 2003 (Cth) and Do Not Call Register Act 2006 (Cth), where applicable to communications
- Fair Work Act 2009 (Cth), applicable industrial instruments and employment-record obligations
- applicable funding agreements, program guidelines, professional obligations, regulator directions and recordkeeping requirements
- Archives Act 1983 (Cth), only to the extent SECC holds Commonwealth records or is otherwise subject to that Act

Approval and Version History

Version	Change	Prepared by	Approved by	Approval date	Next review
3.0	Complete replacement draft – privacy, health information, aged care, data breach and information-governance update	CEO / Privacy Officer	SECC Board	28 September 2026	Within 12 months, then at least every 3 years