

Privacy Policy

Purpose

The purpose of this policy is to outline the privacy practices of Communities at Work including how we collect and manage personal information and how individuals may access, and correct, records containing their personal information, or make a complaint about a breach of privacy.

Introduction

This policy applies to all Communities at Work Personnel (including staff, volunteers, and contractors). This policy covers personal information collected:

- regarding Communities at Work staff, contractors, applicants for employment, and volunteers;
- regarding individuals who access or receive Communities at Work services, their carers or family members and any other person that has contact with the Communities at Work; and
- regarding donors and prospective donor information from third parties for fundraising purposes.

Where a funding agreement has specific requirements pertaining to the collection and storage of sensitive information that are outside of this Policy, a separate procedure or protocol may exist or will be developed as necessary and will be an extension of this Policy.

This policy is consistent with the Privacy Act 1988 and the associated Australian Privacy Principles.

Authorisation

This policy shall be endorsed and issued under authority of the Chief Executive Officer.

Policy

Communities at Work recognises the importance of, and is committed to, protecting an individual's dignity, right to privacy and rights to their personal information.

Communities at Work complies with laws that protect specific types of Personal Information in service delivery to, for example, children, older people, and people with disabilities, as well as federal and state legislation that imposes specific obligations relating to handling Personal Information and Health Information, as applicable to particular Personal Information. These include:

- the Australian Privacy Act 1988 (Cth) (Privacy Act);
- the Australian Privacy Principles (Privacy Principles);
- the Information Privacy Act 2014 (ACT);
- the My Health Records Act 2012 (Cth);
- the Health Records (Privacy and Access) Act 1997 (ACT).

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	1 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

Communities at Work takes reasonable steps to communicate and implement its policies, practices, procedures and systems in compliance with Australian Privacy and Related Laws.

Communities at Work respects the privacy of children and young people, and people living with a disability. Communities at Work takes reasonable steps, including using appropriate language and modes of communication, to ensure that all individuals understand their rights to privacy and confidentiality and that they understand what Personal Information is collected, used, stored, and disclosed, and why.

By providing Personal Information to Communities at Work, individuals consent to the use, storage, and disclosure of that information as described in this Privacy Policy.

Communities at Work acknowledges and supports an individual’s right to complain if they believe their privacy has been breached contrary to this Privacy Policy and to Australian Privacy and Related Laws. The process for making a complaint is set out at Part Complaining about a breach of privacy of this Privacy Policy.

Communities at Work may, from time to time, review and update this Privacy Policy to take into account new laws and technology, changes to our operations and practices and to ensure it remains appropriate to the changing environment in which we operate. Any changes to this Privacy Policy will be notified to individuals by Communities at Work posting an updated version of the Privacy Policy on Communities at Work’s website, with the revised version taking effect from the time it is published.

Personal information that Communities at Work may collect

Communities at Work may collect personal information required to carry out its functions or activities. These include employment, service delivery, referrals, fundraising and communication, complaints handling and reporting. It also includes information that individuals provide to Communities at Work through its websites or online presence. Communities at Work also collects personal information where necessary or required by law.

Communities at Work collects personal information about people we assist:

1. directly with the individual’s consent; or
2. through the individual’s nominated person (such as a carer or family member), partnering service or government agency.

The types of Personal Information Communities at Work may collect includes:

1. Sensitive Information from individuals to provide assistance, including facilitating arrangements with, or on behalf of, individuals for financial assistance, accommodation, community engagement and medical and/or mental health assistance;
2. Personal Information regarding applicants for employment, volunteers, or contractors, including:
 - a. job applications;
 - b. professional development history;
 - c. medical information (for example details of disclosed disabilities and/or allergies, medical certificates);
 - d. emergency and/or family contact information;

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	2 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

- e. workplace surveillance information, including video; work emails and private emails (when using work email address); and Internet browsing history.

Communities at Work may engage third parties to provide limited Personal Information to Communities at Work about individuals for marketing and fundraising purposes.

For other people who come into contact with Communities at Work, Personal Information necessary for the purpose of contact will be collected, for example, name and contact details.

Communities at Work will not record telephone conversations for quality, compliance and training purposes without the express consent of the parties to the call.

Communities at Work may use GPS tracking devices in its vehicles in accordance with relevant legislation.

Sensitive Information

Communities at Work will only collect Sensitive Information with the consent of the individual and where the information is reasonably necessary for it to carry out its functions or activities.

Communities at Work will also limit the use and disclosure of Sensitive Information to instances where the information is:

- directly relevant to the purpose for collection;
- reasonably necessary to carry out its functions or activities; or
- required by law.

Communities at Work will explain the purpose for which Sensitive Information will be used, provide individuals the opportunity to discuss any concerns they may have, and record in Communities at Work Privacy disclosure form (Appendix 1) whether consent was given to use the Sensitive Information.

Purposes for the collection, holding and usage of personal information

Communities at Work collects, holds and uses Personal Information:

- to advise about, assess eligibility for, and provide, Communities at Work services and to meet funding, professional and legal obligations in the provision of services;
- to effectively undertake its business activities and functions, including:
 - keeping individual’s records and contact details up to date;
 - complying with industrial relations, human resources, and workplace health and safety obligations including workplace claims management systems;
 - processing and responding to complaints;
 - marketing and communications;
 - responding to media requests (these are referred to the Media and Communications Team who will comply with the privacy requirements in the Media Policy);
 - organisational planning;
 - service development and quality control;
 - research, monitoring, advocacy and evaluation;

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	3 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

- publishing de-identified Personal Information in submissions and reports;
- meeting funding, audit and regulatory reporting requirements through the provision of de-identified personal information;
- complying with any law or court/tribunal orders;
- complying with regulatory authorities and government requirements, or
- fundraising purposes.

How Communities at Work collects personal information

Communities at Work collects Personal Information (and any Sensitive Information such as health information and probity checks) directly from individuals unless it is unreasonable or impracticable to do so.

As part of its commitment to open and transparent management of personal information, where Communities at Work requires the collection of Personal Information, Communities at Work will advise individuals whether it is possible to interact anonymously or by using a pseudonym. For example, if an individual contacts Communities at Work’s by email or phone with a general question, a name will not be required unless the individual chooses to provide it.

Where anonymous interaction or use of pseudonym is not possible, Communities at Work will advise individuals about their privacy rights including: the purpose for the collection of information; who it may be shared with or disclosed to (where possible); and how it will be stored. This advice will be provided before an individual is asked to consent to the collection or sharing of that information, in language and in a mode that they can understand.

Communities at Work’s first and preferred approach is to collect Personal Information directly from individuals wherever possible and to ensure that they have provided informed consent. Where Communities at Work seeks personal information from individuals who require assistance to provide this information directly, Communities at Work will take the necessary steps to explain the individual’s right to privacy and to obtain consent in accessible format. This may include the use of appropriate written, picture or other format. Communities at Work will record the steps taken to explain and achieve informed consent in the notes of client meetings and store these securely in personal record files.

Communities at Work may also collect Personal Information directly from publicly available sources or from third parties. Third parties may include:

- individual’s carers, guardians, advocates or authorised representatives;
- individual’s medical and/or health professionals;
- government or non-government agencies that Communities at Work partners with to deliver services;
- law enforcement agencies;
- parties to a complaint;
- prescribed bodies permitted to provide Chapter 16A information relating to the safety, welfare and wellbeing of a child or young person; or
- third parties for fundraising purposes.

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	4 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

Where Communities at Work collects Personal Information about an individual from third parties, Communities at Work will take reasonable steps before the time of, or at the time of, collection; or as soon as practicable after collection; to let the individual or their authorised representative know the circumstances of the collection.

When personal information requested is not provided

Individuals can decline to provide Personal Information. However, if the Personal Information requested is not provided Communities at Work may not be able to:

- provide the requested services (or information about those services), either to the same standard or at all;
- engage an individual as a volunteer, employee or contractor;
- employ or enter into a contract with an individual;
- meet funding, professional and legal obligations;
- respond to a complaint, or
- tailor the content of our websites which might impact the experience of our websites.

Disclosure of personal information

Communities at Work may disclose Personal Information to a third party in certain circumstances.

Communities at Work will not disclose Personal Information to another party if an individual explicitly denies consent for the disclosure except where such a disclosure is required by law.

Communities at Work will ensure that any disclosure request is made in writing when possible and practical. If it not possible or practical to obtain a disclosure request in writing, this will be recorded by Communities at Work. While complying with relevant laws, Communities at Work will only disclose such information as is necessary and required, including in accordance with the Personal Information Requests Policy.

Communities at Work may disclose an individual’s Personal Information within Communities at Work or to a third party including:

- contractors;
- suppliers;
- service providers-including those who assist in fundraising strategy, activities, and analysis;
- funders;
- regulators, or
- charities to the extent necessary to effectively undertake its business activities and functions.

From time to time Communities at Work provides some personal information to other charities and data co-ops, based in Australia and subject to Australian Privacy and Related Laws, to increase its donor base.

If Communities at Work provides services to an individual, it may also disclose their Personal, health and Sensitive Information to:

- their authorised representative or advocate;

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	5 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

- other non-government agencies or government agencies that Communities at Work has a partnership with for the delivery of its services;
- members of a health treatment team (including other health service providers involved in diagnosis, care, and treatment) to the extent necessary to improve or maintain their health or manage a disability;
- prescribed bodies where disclosure *or sharing* of information relating to a child or young person’s safety or well-being is *allowed* or required under legislation;
- employees, volunteers, contractors, suppliers, or service providers for the purposes of providing the service;
- courts or tribunals in compliance with Court orders;
- external professional individuals or organisations in circumstances where a Communities at Work employee is subject to external professional supervision or peer review, or
- anyone else for any authorised purpose with the individual’s express consent.

Communities at Work may receive and will comply with disclosure requests regarding information held about individuals, to comply with legal obligations, including:

- pursuant to a court order or subpoena;
- information relating to the safety, welfare and wellbeing of a child or young person under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998 (NSW)*, or under sections 860 to 863A of the *Children and Young People Act 2008 (ACT)*.
- where there is a serious or imminent threat to the life or health of the individual concerned or another person.

Disclosure of personal information to anyone outside Australia

Communities at Work will take reasonable steps to ensure that any disclosure of Personal Information to third parties overseas, including to Communities at Work’s own overseas affiliates, is compliant with Australian Privacy and Related Laws.

Communities at Work’s websites and online presence privacy practices

Communities at Work uses social media platforms such as Facebook to facilitate its business activities and functions and post information about events and activities. Individuals who interact with Communities at Work through these services are responsible for reviewing and accepting their privacy policies prior to interacting with Communities at Work. These services may use cloud-based data storage services. Some of these services and platforms store information overseas. The privacy laws of these countries may not provide the same level of protection as Australian Privacy and Related Laws. Individuals providing information to Communities at Work cannot seek redress against these services under Australian Privacy and Related Laws and may not be able to seek redress overseas.

Communities at Work’s public website (www.commsatwork.org) collects limited generic user information to identify generic user behaviours such as webpages visited and popular content. Where the website allows individuals to make comments, give feedback or make a credit card payment, Communities at Work

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	6 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

may collect email addresses and other contact details. Communities at Work may use email addresses provided to respond to feedback and, on occasion, to make direct contact for surveying purposes and ongoing communication. The Personal Information from the website is stored on servers located in Australia.

Where there is a mailing list that individuals have subscribed to, there will be a simple option available to opt out of receiving further information or correspondence if they no longer wish to receive communication.

If individuals visit the website to read, browse or download information, information such as the date and time of the visit to the website, the pages accessed and any information downloaded may be recorded and used for statistical, reporting and website administration and maintenance purposes.

Communities at Work's website may use 'cookies' (small summary files containing an ID number unique to your computer). Cookies allow Communities at Work's system to identify and interact more effectively with other devices. They help Communities at Work to maintain the continuity of the browsing session, remember the visitor's details and preferences if they return, and to measure traffic patterns to determine which areas of our websites have been visited so that we can improve our services. Our cookies do not collect Personal Information. Individuals can configure the web browser software to reject cookies, however some parts of the website may not have full functionality in that case.

When Communities at Work sends emails or other electronic messages, it may record where the message was opened and what particular links were clicked on to better understand what information is of interest to the viewer.

Communities at Work is subject to laws requiring it to protect the security of Personal Information once it comes into its possession. However, any Personal Information sent through the website or other electronic means may be insecure in transit, particularly where no encryption is used (for example email or standard HTTP). The website may contain links to other sites operated by third parties. Third party websites are responsible for informing you about their own privacy practices and Communities at Work is not responsible for the privacy practices or policies of those sites.

Communities at Work may log IP addresses (that is, the electronic addresses of computers connected to the internet) to analyse trends, administer the websites, track users' movements, and gather broad demographic information.

Communities at Work engages external data aggregators including Facebook and Google Analytics to identify individuals who may be interested in Communities at Work campaigns and activities, based on their usage of Communities at Work's website. Communities at Work uses Google Analytics to inform and optimise content based on an individual's past visits to Communities at Work websites. Google Analytics informs Communities at Work how visitors use the websites based on their browsing habits, so that Communities at Work can improve its websites, and make it easier to find information. Google also receives this information as individuals browse Communities at Work's websites and other websites on the Google Display Network using Remarketing. Individuals can opt-out of customised Google Display Network services and Google Analytics for Display Advertising using ad settings and can use the Google Analytics Opt-out Browser Add-on to not be tracked into Google Analytics.

Despite all precautions taken by Communities at Work to protect Personal Information, because our websites are linked to the Internet, we cannot provide any assurance regarding the security of any transmission of information individuals communicate online. Communities at Work also cannot guarantee

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	7 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

that information supplied will not be intercepted while being transmitted over the internet. Accordingly, any Personal Information or other information transmitted to Communities at Work online is transmitted at the individual's own risk.

Storage, security and accuracy of personal information

Communities at Work will take reasonable steps to ensure that Personal Information collected, stored, used and disclosed by is accurate, complete and up-to-date. Communities at Work will also take reasonable steps to ensure that Personal Information used and disclosed by is relevant, having regard to the purpose of the use or disclosure. To ensure this Communities at Work will:

- aim to record information in a consistent format;
- where necessary and/or possible, confirm the accuracy of the information collected from a third party or a public source;
- promptly add updated or new personal information to existing records, and
- review the quality of personal information before it is used or disclosed.

Communities at Work takes reasonable steps to ensure Personal Information is protected from misuse, interference, loss and unauthorised access, modification, or disclosure. Personal Information in electronic form is stored in electronic databases that require passwords and logins.

Personal Information in hard copy is kept securely. Communities at Work's standard practice is to destroy or de-identify records of Personal Information once they are no longer needed. If Communities at Work is required to disclose Personal Information, it will take reasonable steps to prevent unauthorised use or disclosure of that information.

Communities at Work does not use any government assigned identifier as a primary form of identification, such as an individual's Tax File Number or Medicare Number. Communities at Work takes reasonable steps to ensure that the Personal and Sensitive Information relating to individuals is de-identified, particularly when such information is required for reporting or other statistical purposes.

Where Communities at Work must request information from Centrelink to check eligibility for concessions, rebates, and services it will only utilise the information to the extent necessary to perform the required services.

Storage and security of credit card information

Communities at Work may collect and use information from credit card transactions only for business purposes. These business purposes may vary depending upon the circumstances. The credit card information provided to Communities at Work will be stored in a confidential manner, normally through our SharePoint platform. Communities at Work employees may access such information only when there is an appropriate business reason to do so, such as when a refund must be issued back to the credit card. Communities at Work will maintain appropriate physical, electronic and procedure safeguards to protect your financial information, and our employees are required to follow these privacy standards.

Retention and destruction of personal information

Communities at Work complies with requirements under the Archives Act 1983 (Cth) and its own Records Retention Policy, to protect personal information it holds. Generally, Communities at Work is required to keep records for a minimum of seven years from the date it was last accessed or until the relevant individual has reached 25 years of age, whichever is longer. In addition, Communities at Work has a restricted access system where only appropriate Communities at Work Personnel have access to files.

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	8 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

Communities at Work protects information held from both internal and external threats by:

- regularly assessing the risk of misuse, interference, loss and unauthorised access, modification or disclosure of that information;
- taking measures to address those risks, for example, by keeping a record (audit trail) of when someone has added, changed or deleted Personal Information held by Communities at Work electronically, and
- maintaining electronic security of Communities at Work premises and information systems, including password protection for electronic files (further, Communities at Work’s internal network and databases are protected using firewall, intrusion detection and other technologies).

Accessing and correcting personal information

Where individuals or their nominated person and Communities at Work agree that changes to Personal Information held by Communities at Work need updating or amendment, changes to records containing that information will be made following an informal request.

Individuals or their nominated person may request formal access to their personal information held by Communities at Work at any time by making a written request to the Chief Executive Officer, Communities at Work by:

Post: PO Box 1066 Tuggeranong ACT 2901

Email: privacy@commsatwork.org

After Communities at Work has established the appropriate personal identification of the individual and if applicable, the requisite authority of the nominated person, Communities at Work will usually make the requested information available for inspection within 28 days upon receipt of the request for access. Some services may have additional requirements relating to access (such as requiring individuals to view files in person with an employee of Communities at Work present to provide additional support or information).

Communities at Work may refuse access where it reasonably believes that granting access would pose a serious threat to the life, health, or safety of an individual or to public health and safety, have an unreasonable impact on the privacy of another individual or if it would result in a breach of confidentiality. Where Communities at Work refuses access, it will give written reasons. Where Communities at Work refuses access to Personal Information on the ground that it would present a serious threat to an individual’s life or health, an individual may request Communities at Work to provide access through an intermediary (such as a treating medical practitioner) who would consider whether access should be provided.

Individuals or their nominated person can make a request in writing to amend Personal Information held by Communities at Work if they believe the Personal Information held by Communities at Work is inaccurate, out-of-date, misleading, or incomplete.

If an individual believes that the Personal Information Communities at Work holds about them is incorrect, incomplete, out-dated, or inaccurate, they may request Communities at Work to amend it. The request will be treated confidentially. In responding to the request, Communities at Work will:

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	9 of 14

MASTER DOCUMENT – UNCONTROLLED WHEN PRINTED UNLESS SIGNED IN RED

- consider if the information requires amendment;
- if it agrees that the information require amendment, correct the information as soon as practicable and notify the individual that the changes have been made in accordance with the Records Management Policy;
- if it does not agree that there are grounds for amendment, provide notification in writing of the reasons for the declined request, referencing laws where applicable that permit, or
- require Communities at Work not to approve the request (Communities at Work will also provide notification of any available avenues for review of the refusal and will add a note to the personal information indicating that the individual has requested that the information is amended).

Privacy and data breaches

Despite Communities at Work’s best efforts to protect and safeguard individuals’ privacy, information data breaches may occur including:

- unauthorised access (including by staff, volunteers, contractors or external third parties such as by hacking);
- unauthorised disclosure (whether intentional or unintentional through human error – for example a staff member accidentally sends Personal Information of individuals accessing a particular service to the wrong email address); or
- loss or theft (for example, hard copies of documents, electronic devices and storage devices being misplaced or stolen).

Communities at Work must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of ‘eligible data breaches’ when:

- there is unauthorised access to, or unauthorised disclosure of, personal information, or loss of personal information;
- unauthorised access to or disclosure of personal information is likely to result in serious harm to one or more individuals; or
- efforts to contain the harm with remedial action have been unsuccessful.

In these circumstances Communities at Work must notify the OAIC, the affected individuals and funding body (as applicable) of: the contact details of Communities at Work; a description of the eligible data breach; the kinds of information concerned (for example, health records, sensitive information); and recommended steps individuals can take relating to the breach.

When notifying individuals, Communities at Work will, depending on the most appropriate course, either notify all affected individuals; or notify only those individuals at risk of serious harm; or if those options are not feasible, publish a Notifiable Data Breach statement on Communities at Work website and publicise it. Where Communities at Work is required to also report the breach to other enforcement agencies, it will take reasonable steps to inform individuals concerned.

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	10 of 14

Complaining about a breach of privacy

Individuals, or their authorised representative, with any questions or concerns regarding a possible privacy breach, should contact Communities at Work’s Privacy Officer who will confidentially discuss the concerns and outline options for resolution.

Communities at Work recognises the right of all individuals, or their authorised representative, to complain about possible privacy breaches by Communities at Work.

Communities at Work will provide a procedure to receive and resolve complaints fairly and accessibly, in a timely manner that is procedurally fair, without reprisal for the person making the complaint.

Communities at Work acknowledges the right of individuals to be represented by an authorised representative or advocate of their choice at all stages of the complaint process and will inform the individual of this at the time they make a complaint.

Where an individual is not represented and requires support to make a complaint, Communities at Work will ensure that appropriate support and assistance is provided to them to do so.

Individuals, or their authorised representative, wishing to make a complaint to Communities at Work regarding the handling of personal information, can do so via:

Post: PO Box 1066 Tuggeranong ACT 2901

Email: privacy@commsatwork.org

Phone: 02 6293 6500 (ask for the Privacy Officer), or by other modes that are appropriate in the circumstances.

Communities at Work will aim to resolve complaints in a timely, satisfactory, fair and transparent manner in accordance with Communities at Work’s Complaint Handling Policy.

However, where individuals are not satisfied with the results of the complaint, depending on the nature of the complaint, they or their nominated person can make a complaint to the Office of the Australian Information Commissioner via:

Post: GPO Box 5218 Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

or to the NDIS Quality and Safeguards Commission via:

Post: PO Box 210 Penrith NSW 2750

Email: contactcentre@ndiscommission.gov.au

Phone: 1800 035 544

1800 880 052 (National Disability Abuse and Neglect Hotline) or to the ACT Ombudsman via:

Phone: (02) 6276 0111

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	11 of 14

Definitions

Australian Privacy and Related Laws	The laws relating to management of Personal Information applicable to Communities at Work set out at Part 4 of this Privacy Policy.
Personal Information	Any information or opinion about an individual who is reasonably identifiable.
Privacy Act	The Privacy Act 1988 (Cth)
Privacy Principles	The Australian Privacy Principles at Schedule 1 of the Privacy Act
Sensitive Information	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, criminal record or physical or mental health.

Responsibilities

Communities at Work CEO

- Responsibility for any amendments to this policy rests with the CEO in consultation with senior management.
- Reporting to the Communities at Work Board breaches of privacy.

Privacy Officer

- Providing internal privacy advice. This may be about upcoming projects involving the handling of personal information, or in response to ad hoc enquiries from Communities at Work employees, volunteers or contractors about how they should handle personal information.
- Assisting colleagues with the completion of privacy impact assessments for proposed initiatives involving the handling of personal information.
- Co-ordinating Communities at Work’s response to suspected or confirmed data breaches.
- Responding to queries about Communities at Work’s privacy practices from members of the public.
- Handling privacy complaints that Communities at Work receives directly. This may include investigating whether Communities at Work has interfered with someone’s privacy and trying to resolve the complaint.
- Liaising with OIAC and other relevant privacy regulators about data breach notifications, privacy complaints or significant projects.
- Assessing whether requests from other organisations to share personal information that Communities at Work holds are permitted under privacy law.

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	12 of 14

Executive:

- Have the responsibility to ensure that this policy is implemented within their program areas and incorporated into their team’s practices as necessary.
- Provide adequate support and direction to key personnel responsible for handling reports of suspected privacy breaches.
- Where a funding agreement has specific requirements pertaining to the collection and storage of sensitive information that are outside of this Policy, a separate procedure or protocol may exist or will be developed as necessary and will be an extension of this Policy.

Employee:

- Be aware of the Privacy Policy and procedures.
- Undertake all assigned Privacy training as directed.

Attachments & Forms

1. Get In Touch

Related Documents:

1. ORG-QMS-POL-001 Purpose, Mission and Values
2. ORG-QMS-POL-009 Records Management Policy
3. ORG-QMS-POL-010 Management Responsibilities, Review and Planning
4. ORG-QMS-POL-023 Continuous Improvement Policy
5. ORG-QMS-PRO-001 Complaints Management Policy
6. ORG-QMS-POL-060 Grievance Management Policy
7. ORG-QMS-POL-114 Incident Response and Crisis Management Policy
8. ORG-QMS-POL-108 Information Security Policy
9. ORG-QMS-POL-046 Data Management Policy
10. ORG-QMS-POL-080 Database Access Policy
11. ORG-QMS-POL-121 Cybersecurity Governance and Management Policy
12. ORG-QMS-POL046 Disaster Recovery Policy
13. ORG-QMS-PRO-004 Corrective and Preventative Action Procedure
14. ORG-QMS-PRO-007 Incident Reporting Procedure
15. ORG-QMS-PRO-001 Complaints Management Procedure
16. ORG-QMS-PRO-174 Incident Reporting (Cyber Security) and Response Plan

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	13 of 14

References

1. ISO 9001:2015 Quality Management System
2. ISO 3100: 2018 Risk Management
3. AS ISO/IEC 27004:2018 Information Security Management

Document Contact

GRC Administration

P: 02 6293 6500

E: grc@commsatwork.org

Review Specifications

OFFICE USE ONLY			
Written/reviewed by	Authorised for release by	Version number	Signature of authorising person
Michelle Colefax	Michelle Colefax	6.0	Michelle Colefax
VERSION HISTORY			
Version:	Date of Effect:	Brief Summary of Change:	
V1.0	10 October 2013	Presented to Quality Committee for endorsement	
V2.0	12 March 2014	Update with release of amendments to Privacy Act	
V3.0	16 June 2015	Revised and reformatted	
V3.1	29 April 2016	Formatting to comply with Style Guide, Control Copy required and update of Authorised Signatory	
V4.0	24 January 2017	Reviewed and updated	
V5.0	22 February 2018	Handling of Personal Information Notifiable Data Breaches Scheme	
V5.1	January 2019	Annual review and reissue, replacing Disability Services with Lifestyle Services in Retention period table.	
V5.2	7 June 2019	Specifying 'contractors' as 'other person' covered by this policy.	
V5.3	12 June 2019	Typos, incorporated Incident Response Plan in Related Documents, ISO standard updated and document contact email updated.	
V6.0	28 February 2024	Policy rewritten.	

Document Type	Doc Ref No	Version No	Date of Effect	Due for Review	Page
Policy	ORG-QMS-POL-002	V6.0	28/02/2024	28/02/2027	14 of 14