Privacy Management and Confidentiality Policy

Purpose

This policy defines the manner in which Communities@Work collects and manages personal information supplied by individuals through processes established to facilitate the efficient and responsible operation of the organisation. This policy includes provisions for privacy protection for individuals supplying information to the organisation, and confidentiality agreements to protect the integrity of information entrusted to, and managed by, Communities@Work.

Introduction

This privacy management and confidentiality policy is important to the organisation because it relates to an individual's physical and moral autonomy and Communities@Work's moral obligations as a community sector organisation.

Communities@Work is strongly committed to protecting the privacy of its staff, volunteers, clients and stakeholders and respecting the confidentiality of information provided to the organisation.

Communities@Work aims to collect and manage an individual's information in a manner that is transparent and conducive to the regulatory environment in which it operates. In all circumstances, we will take all reasonable steps to secure the confidentiality of information provided to us.

Australian Privacy Principles (APPs) dictate minimum requirements that must be met by law to ensure appropriate management of personal and sensitive information that Communities@Work receives and uses. This document outlines how Communities@Work manages such information in accordance with the APPs.

This policy framework is consistent with the Privacy act 1988 and the associated Australian Privacy Principals

Authorisation

This policy shall be endorsed and issued under the authority of the Chief Executive Officer. The Chief Executive Officer may authorise amendments to this policy at any time.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

Policy

Communities@Work will implement and maintain practices and procedures to regulate the collection and management of personal information to ensure compliance with the thirteen (13) Australian Privacy Principles outlined in the Privacy Act 1988.

Employees, volunteers and other persons (including contractors) engaged in work practices involving the handling or management of personal or other sensitive information on behalf of Communities@Work found to be in breach of this policy, supportive procedure or legal obligations may face disciplinary action up to and including termination.

Information this policy applies to

Communities@Work has a responsibility to protect all personal or sensitive information that is provided during the course of carrying out its operations. The organisation is committed to, and legally obligated to, ensure the privacy of information provided by:

- recipients of a service or participants in a program owned or managed by Communities@Work; or
- employees, volunteers, or other individuals (prospective, new or existing) who seek to be engaged in any work capacity by Communities@Work (other individuals may include agency employees, students, consultants, contractors or allied professionals).

The types of personal or sensitive information that may be entrusted to Communities@Work include, for example:

- information collected through documented procedures and programs established by Communities@Work to meet performance requirements, government reporting requirements, legal/regulatory requirements and security requirements;
- details of financial and commercials transactions; or
- worker's compensation or relevant functional assessment or medical information relating to the employment relationship.

Collecting information

Communities@Work must collect personal or sensitive information about individuals for a variety of purposes such as delivering services, or engaging employees and volunteers.

Information may be solicited – for example, the information is requested by Communities@Work to enable Communities@Work employees to deliver a service to the individual.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

Some information may be unsolicited – for example, an individual makes a donation to Communities@Work which includes their name and address for receipt purposes.

When collecting information, Communities@Work employees or volunteers must ensure the following conditions are met:

- personal or sensitive information being collected must be reasonably necessary for the functions or activities of Communities@Work;
- an individual must consent to the collection of their sensitive information - sensitive information may also be collected if it is required by an Australian law or court order;
- information must be collected by lawful and fair means;
- information must be collected from the individual - exceptions may occur where it is unreasonable or impracticable to do so;
- The individual from which information is being collected must be notified at the time of collection, or soon as possible after the information is collected, of:
  - the contact details of Communities@Work
  - why the information is being collected
  - the consequences of some or all of the information not being provided;
  - the details of, or a copy of, Communities@Work's Privacy Policy statement.

It is the responsibility of Communities@Work to ensure that the personal information it collects is accurate and up-to-date. This is done by confirming information with clients when they contact the organisation. Employees or volunteers are requested to notify Human Resources of changes to their information by completing and lodging the (change your details) form.

The Communities@Work Privacy Policy statement contains information for individuals who would like to check or make changes to their personal or sensitive information.

Providing information anonymously

Some individuals may not want their identity known (for example donors) or may wish to use a pseudonym. Where a client accessing our services does not wish to be directly identified, Communities@Work systems must be able to support this request.

The exception is where an Australian law or court order exists requiring Communities@Work to deal with individuals who identify themselves, or where it is impracticable to deal with someone who does not want to be identified.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

Accessing personal information by individuals

In general circumstances, Communities@Work is required to allow individuals access to what information is held about them. The requested information must be provided within a reasonable timeframe.

Individuals have the right to ask for their personal information to be amended if they believe the information is incomplete, incorrect, out of date or misleading. This also applies to personal information that has been or is being used, or is available for use, for an administrative purpose.

Circumstances may exist where there is negative ramifications in disclosing information to an individual. Where a Communities@Work employee believes such a situation exists, they should contact their Branch Manager and refer to the Australian Privacy Principles for guidance. The individual must be given written advice if Communities@Work is unable to meet their request.

Communities@Work does not charge individuals for accessing their information.

Using personal or sensitive information - generally

Information collected from an individual must only be used for the purpose for which it was obtained, unless the individual has consented to the use of the information for other specific purposes.

Disclosure

Communities@Work will only use personal information for the purposes for which it was given to us, or for purposes which are directly related to one of our functions or activities. We will not use or disclose personal information for other purposes unless:

- the individual has consented; or
- the individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, bodies or agencies; or
- it is otherwise required or authorised by law; or
- on reasonable grounds it is believed that it will prevent or lessen a serious and imminent threat to somebody's life, health or safety or serious threat to public health or public safety; or
- the individual has made threats to harm third parties; or
- the individual has made threats against Communities@Work, its staff, volunteers and/or clients, or;
- the individual repeatedly makes nuisance contact including calls, chats or emails.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

Communities@Work will also use disclose information to a law enforcement body (for example, the police) if it is believed that it is reasonably necessary for an enforcement related activity (for example, investigating a crime).

Because Communities@Work offers programs and services to families, we collect personal information about children that may be accessed by parents or carers on the child's behalf.

Information collected by Communities@Work may also be used for quality assurance, research for service improvement, community promotion of Communities@Work services (for example, Communities@Work may use positive feedback on our service to promote services online or via social media) and/or fundraising purposes. However, information will always be de-identified prior to such uses.

Verbal communication of sensitive information - containment

Communities@Work staff are cognizant of the requirement that conversations regarding an individual's private information should not be carried out where they may be overheard by unauthorised person/s. This includes discussing an individual's private information in public places.

Records Management

All records collected by Communities@Work will be retained, managed and destroyed in accordance with regulatory requirements, applicable standards and codes, and the organisational records management policy and procedures.

Records shall be easily accessible and/or retrievable in the event they are needed for any purpose including internal review, audit, litigation or destruction.

Records shall be stored in a manner that gives appropriate consideration to the sensitivity of information and related security provisions e.g. safeguarded against unauthorised access where required by law.

Legally mandated records shall be identified to known users, Program Area Managers and Directors. This information shall be identified and documented in specific program area documentation.

Disposal of records including those flagged for archiving shall be processed in accordance with relevant laws, regulations and requirements documented in the organisation's Quality Management System.

The disposal of records shall be authorised by the records management representative nominated by the organisation or by the CEO or any other person appropriately authorised by the CEO.

Where digital records are used by the organisation, the structure and content must be preserved and protected to ensure authenticity, accuracy and reliability of the records.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

Storage & Handling:

Directors are responsible for the management of Record Archiving for their business unit. Records that are required for regular access are to be stored locally, while records that are not required on a regular basis are to be stored in the organisational off-site storage site (Grace) in accordance with the Minimum Period of Retention.

Directors are responsible for the management of Record Archiving for their business unit. Records that are required for regular access are to be stored locally, while records that are not required on a regular basis are to be stored in the organisational off-site storage site (Grace) in accordance with the Minimum Period of Retention.

Disposition:

Disposition of records should only occur when the following criteria have been met:

- There is no work outstanding; and
- There is no outstanding or pending investigation or litigation related to that record.

Disposition methods include the following:

- Physical destruction, including the deletion or overwriting of electronic data;
- Transfer to another organisation;
- Transfer within Communities@Work; and
- Transfer to the archives.

The criteria for physical destruction of records include:

- The destruction should be authorised by the relevant Director;
- Records pertaining to pending, possible or actual litigation or investigation should not be destroyed;
- Destruction is to occur in a manner that preserves any confidentiality;
- All copies of the records that are authorised for destruction should also be disposed; and
- The record is out of the required retention time required, as per these guidelines.

Minimum Period of Retention:

The following table outlines the minimum period of retention for records at Communities@Work.

Program Area	Record Type	Minimum Retention Period
Governance	Complaints Register	10 years
	Complaint Investigations	10 years
	Incident Reports	6 years
	CAPA	6 years
	Internal Audit Reports	6 years
	External Audit Reports	6 years
	Contracts	6 years after the end of the contract
Professional Services Team	Meeting Minutes	10 years
	Surveys	5 years
	Annual Returns	7 years
	Payroll	7 years
	Personnel	7 years after the termination of an employee
	Worker's Compensation	25 years
Volunteers	Personal details	2 years
	Insurance Matters	7 years
	Compensation Matters	75 years
Children's Services	Attendance Rolls	3 full financial years after child's last attendance

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

	Child Assessment	3 full financial years after child's last attendance
	Incident, Injury Trauma and Illness Record	Until child is 25 years of age
	Medication record	3 full financial years after child's last attendance
	Child Enrolment	3 full financial years after child's last attendance
	Death of a Child	7 years from child's death
	Child Care Benefit	3 full financial years after child's last attendance
Lifestyle Services	Attendance	5 years
	Behaviour	5 years
	Correspondence	5 years
	Medication	7 years
Registered Training Organisation	All	30 years
Parenting Matters	Client Files	5 years

Handling of Personal Information

Communities@Work maintains personal information security as per Australian Privacy Principle 11, including complying with the Notifiable Data Breaches (NDB) Scheme.

In line with the requirements of NDB scheme, we have to set out the procedure and clear lines of authority for Communities@Work staff in the event that the organisation experiences a data breach (or suspects that a data breach has occurred).

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

As per this Scheme we take reasonable steps to ensure an assessment of eligible data breaches is completed within 30 days. We recognise eligible data breach as one that meets the following three criteria:

i. There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information that we hold

ii. The above is likely to result in serious hard (psychological, emotional physical, reputational, or other forms of harm) to one or more individuals

iii. We are unable to prevent the likely risk of serious harm with remedial action.

If an eligible data breach is confirmed, as soon as practicable we provide a statement to each of the individuals whose data was breached or who are at risk, including details of the breach and recommendations of the steps individuals should take.

We also send a copy of the statement to the Office of the Australian Information Commissioner

We undertake a review of how the breach occurred and enhancement to security measures to protect personal information, necessitated by such an event.

Using personal information – direct marketing

Personal information of an individual may only be used for direct marketing purposes where:

- Communities@Work has obtained the personal information from the individual;
- the individual is aware that the information may be used for direct marketing purposes;
- there is an opt-out mechanism for the individual; and
- the individual has not requested to opt out of direct marketing.

Communities@Work must not use personal information for direct marketing purposes where conditions under the *Do Not Call Register Act 2006* or the *Spam Act 2003* apply.

Using personal or sensitive information – overseas

Communities@Work does not disclose personal information about an individual to overseas recipients. If such a need arises, authority must be obtained from the CEO and the requirements of the Australian Privacy Principles must be met.

Using personal or sensitive information – government identifiers

Communities@Work does not adopt government identifiers of individuals, for whom Communities@Work provides services, as identifiers in its own systems. Examples of government identifiers include Medicare numbers, driver's license numbers and tax files numbers.

Communities@Work may only use or disclose government related identifiers where it is necessary to deliver services or comply with state, territory or government requirements.

Secure handling of personal information

It is the responsibility of Communities@Work employees and volunteers to ensure that personal information is not lost or misused. Communities@Work systems must limit access to personal information to those employees or volunteers that need to use the information.

All employees, volunteers and other persons to be engaged in work practices involving the handling or management of personal or other sensitive information on behalf of Communities@Work are expected to sign the organisation's Cultural Code and Confidentiality Agreement in your employment contract prior to commencement.

Communities@Work employees must ensure that computer systems are appropriately backed up and that hard copies of personal information are safely stored at all times

When personal information is no longer required, and is not required to be maintained by a Commonwealth agency or Australian Law, then the information must be destroyed or de-identified.

Complaints

If any individual is not satisfied with the way Communites@Work has collected, managed, used, updated, stored or disposed of their personal information, they may lodge a complaint with Communities@Work. Communities@Work has adopted and documented the following policy on feedback management to meet organisational, regulatory and client requirements.

- All feedback received via the Communities@Work website (https://commsatwork.org/about-us/contact-us/), shall be acknowledged, reviewed, processed and where warranted investigated in accordance with the Complaints Policy and associated procedures.

In the event a complaint cannot be resolved to the satisfaction of the complainant, Communities@Work will provide the complainant with contact information for the Office of the Australian Information Commissioner to access external complaints processes.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

Intellectual Property

All information and intellectual property disclosed or developed by employees, volunteers and other persons engaged in work on behalf of Communities@Work whilst in their employ shall remain confidential and the intellectual property of Communities@Work unless authorised in writing by the Chief Executive Officer, Communities@Work. This clause bears the same relevance to personnel who have ceased a working partnership with Communities@Work.

Definitions

Privacy	Relates to an individual's ability to control the extent to which personal information, enabling identification, is available to others.
Confidentiality	An obligation that restricts an agency from using or disclosing any information in a way that is contrary to the interests of the person or organisation that provided it.
Information Management	For the purpose of this policy the "management" of information shall be a collective term of reference that includes use, storage, security and disclosure.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Sensitive information	(a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

Responsibilities

Communities at Work CEO:

- Responsibility for any amendments to this policy rests with the CEO in consultation with senior management.

Executives and managers:

- Have the responsibility to ensure that this policy is implemented within their program areas and incorporated into their team's practices as necessary.

Attachments & Forms

1. Communities@Work Privacy Policy and Summary of Australian Privacy Principles
2. Communities@Work Confidentiality Agreement.

Related Documents:

ORG-QMS-POL-001	Vision, Mission and Values Statement
ORG-QMS-POL-003	Cultural Code Policy
ORG-QMS-POL-009	Records Management Policy
ORG-QMS-POL-030	Records Management System Guidelines
ORG-QMS-POL-022	Complaints Management Policy
ORG-QMS-POL-029	Governing Legislation List
ORG-QMS-POL-174	Incident Response Plan

References

1. *Do Not Call Register Act 2006*
2. *Spam Act 2003*
3. *Privacy Act 1988*

4. Australian Privacy Principles
5. Rights and Responsibilities under the Privacy Act
6. Australian Privacy Principles Guidelines
7. Privacy Regulations
8. Notifiable Data Breaches Scheme
9. ISO 9001:2015
10. ISO 15489-1:2001(E) Information and Documentation – Records 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**
Pankaj Popli	Lee Maiden	V5.3	

VERISON HISTORY		
Version:	**Date of Effect:**	**Brief Summary of Change:**
V1	10 Oct 2013	Presented to Quality Committee for endorsement
V2	12 Mar 2014	Update with release of amendments to Privacy Act
V3	16 Jun 2015	Revised and Reformatted
V3.1	29 Apr 2016	Formatting to comply with Style Guide, Control Copy required and update of Authorised Signatory
V4	24 Jan 2017	Reviewed and Updated
V5	22 Feb 2018	Handling of Personal Information- Notifiable Data Breaches Scheme
V5.1	Jan 2019	Annual review and reissue, replacing Disability Services with Lifestyle Services in Retention period table.

v5.2	07.JUNE.2019	Specifying 'contractors' as 'other person' covered by this policy.
5.3	12 JUNE 2019	Typos, incorporated Incident Response Plan in Related Documents, ISO standard updated and document contact email updated.

02 6293 6500 | admin@commsawork.org | PO Box 1066 Tuggeranong ACT 2901 | ABN 19 125 799 859 | commsatwork.org