Privacy Policy

Person responsible for review: Manager Quality, Risk and Safety

1.0 Introduction

ACSO and McCormack Housing acknowledges that privacy is a fundamental human right and has a legal and ethical obligation to protect our clients right to privacy. ACSO and McCormack Housing provides a range of services, such as assessments, counselling, case work and residential services. In order to provide these services effectively, we need to collect personal information of those accessing our services such as name, address and telephone number. We also need to collect sensitive information such as details about health and background information which help us to understand service needs. The purpose of this policy is to outline the Group's management of client personal and sensitive information.

This policy applies to all personal information about clients collected, used, stored and destroyed by ACSO and McCormack Housing (electronic or hard copy).

Throughout this policy, 'personal information' will refer to personal and sensitive information.

This policy will guide the collection, use, storage and disposal of client personal information held by ACSO and McCormack Housing to ensure our practices comply with privacy laws, contractual obligations and maintain confidence with our external stakeholders.

2.0 Scope

All ACSO and McCormack Housing employees, contractors, volunteers and students (personnel) must comply with this Privacy Policy at all times, regardless of location where work related duties are being performed. For example, working from an ACSO office, a Prison or working from home. All privacy related policies, procedures, processes and statements are to comply with this Privacy Policy.

3.0 Definitions

Privacy	Refers to personal information that is held by ACSO and is protected from unauthorised access or disclosure. It is information given to ACSO / McCormack Housing under an obligation not to disclose that information to others unless there is a statutory requirement or duty of care obligation to do so.
Personal information	Defined in the *Privacy Act 1988* (Privacy Act) as information or an opinion about an identified individual, or an individual who is reasonably identifiable: • whether the information or opinion is true or not; and

	• whether the information or opinion is recorded in a material form or not. For example: a person's name, address, marital status or family history.
Sensitive information	A subset of personal information and is defined as information or an opinion (that is also personal information) about an individual that includes race or ethnic origin, offending history, sexual preference, religious beliefs or affiliations or health information.
Informed consent	Obtaining permission before information is obtained, used or shared. It is giving the client clear and understandable information about the type of personal information that will be requested for collection, how it will be used and stored so the client can decide what information they would like to share and give consent in full knowledge of the possible outcomes by providing their personal information

4.0 Roles and Responsibilities

ACSO Board and Executive team	Responsible for ensuring this policy is implemented at an organisational level.
Senior Leadership team	Responsible for ensuring this policy is implemented at a program level.
Leadership team (Program Managers and Team Leaders)	• Promoting the rights of client's privacy in line with all privacy policies and procedures. • Ensuring ACSO personnel follow the privacy policies and procedures. • Reporting on privacy breaches raised through their services • In consultation with the Privacy Officer, assisting in responding to privacy queries, complaints and breaches and making recommendations and providing advice to the CEO and where necessary the Board and Board Committee. • Using trend data to identify and act upon opportunities for service improvements
Privacy Officers (Quality and Risk)	Responsible for monitoring and reviewing privacy related processes in ACSO services which includes: • Providing consultation stakeholders regarding privacy related matters and best practice. • Ensuring clients privacy is managed according to Privacy Policy • Leading any response to privacy about ACSO services determined, making recommendations and providing advice to the CEO and where necessary the Board and Board Committees.
ACSO Employees	• Promoting the rights of client's privacy in line with all privacy policies and procedures. • Ensuring that the privacy, confidentiality and dignity of clients is maintained at all times. • Ensuing compliance with all ACSO privacy policies and procedures. • Ensuring that clients are aware of their right to access their personal information and make a privacy complaint • Ensuring potential or actual privacy breaches are reported to leaders immediately. • If necessary and appropriate, assisting a client to make a privacy

	complaint. • Collect client personal information only that is relevant to the provision of assistance to the person concerned.

5.0 Workplace Privacy Guidelines

5.1 ACSO Employees Privacy

ECV personal information which relates to their employment with ACSO or McCormack Housing is exempt from the Privacy Act. ACSO will, however, collect, use, store and destroy the personal information of ECV in a manner that aligns with the Australian Privacy Principles (APP's), which underpin the Privacy Act. ACSO will only collect, access and store ECV personal information when it is necessary and related to employment purposes. There may be times where ACSO is required to share the personal information of ECV's with an external government, company or statutory body such as FairWork to establish that ACSO is meeting its employment obligations, under the Fair Work Act 2009. Information that directly relates to the employment relationship can include things such as the ECV's skills, performance, conduct, and their terms of employment.

5.2 Working from Home Standards

Working from home can pose increased or new types of privacy risks, such as those we share our homes with being able to view personal and sensitive information where workstations are not set up in a secure setting. To mitigate the risks of privacy breaches and to ensure cyber safety when working from home, ACSO personnel must continue to work in accordance with all aspects of this policy to ensure personal and sensitive information is protected against unauthorised access.

As hubs are accessed, ACSO personnel may operate from two work places; home and a hub. At all times, ACSO expects ACSO personnel to comply with this Privacy Policy. ACSO personnel must familiarise themselves with section 6.2 Clean Desk Policy and it's supporting resource 'Maintaining Privacy and Information Security: 7 practical guidelines for maintaining a clean desk' to help implement best practice privacy skills and awareness into their roles.

6.0 Policy Implementation Guidelines

6.1 Collection and Use of Personal Information

To provide services, ACSO may only collect and use client personal information for the purposes for which it has been collected, the type of information may include:

- Identifying information such as name, address, telephone number, place and date of birth,

gender, nationality, ethnicity, language spoken

- Next of kin details, including place and date of birth of parents and siblings, family and relationship background information, name and contact details for significant others, guardianship information.
- Accommodation and respite support details, carer's details and transport requirements.
- Billing details for payment
- Sensitive information such as support requested and provided, psychosocial history, counselling reports, court reports, behavioural history, likes and dislikes and interests, photos and videos of activities, assessment and therapy sessions.
- Special needs information including type, extent and support required, need assessment information, health details including medical records, medical summaries, medication reviews and history, and daily activity reports
- Program specific paperwork, forms and reports.
- The purposes for collecting and using client personal information may include:
- Providing a service to a client
- Referral other organisation's services
- Assessment of support needs
- Risk reduction
- Incident management and reporting
- Service planning and improvement

6.2 Consent to Collect and Use Personal Information

ACSO may only collect, use or discloses personal information it has collected and holds, for the primary purpose in which it was collected, where there is client consent. For example, to provide a service

Personal information may be used or disclosed for a secondary purpose when;

- A client consents and it is authorised or permitted by law
- Where the client would reasonably expect the use or disclosure of the secondary purpose
- Where it is related to the primary purpose
- It is permitted to do so by an exception under the relevant privacy laws. For example, use or disclosure may be permitted where it is reasonably necessary to lessen or prevent a serious or imminent threat to an individual's life, health safety or welfare.
- Unlawful activity or serious misconduct has occurred or alleged

ACSO collects personal information through fair and lawful means and must be collected from the client directly, unless this is unreasonable or impracticable. Where this can't occur, personal information must be collected in ways associated to service delivery. For example, via referral information or the clients care team.

Where client personal information is collected from someone else (where there is client consent or permitted by privacy based laws), ACSO will take reasonable steps to ensure that the client is informed of the personal information collected and the circumstances of the collection. Clients do not need to be informed where so would pose a serious threat to the life or health of any individual or would involve the disclosure of information given in confidence. There are circumstances where federal, state and territory privacy laws require or allow ACSO to obtain or share sharing without client consent.

6.3 Informed Consent

Informed consent, in writing or verbal, must be obtained from clients engaging in ACSO's services at first contact, in order to collect and use their information, and to share their information with other services and agencies. Only then will essential and relevant details be shared.

ACSO are to provide the following information to clients about the way ACSO uses and stores their information:

- Purpose of collecting their client information and how it will be used, including whom ACSO will share the information.
- That consent is voluntary and can be withdrawn at any time.
- Limits to privacy of client information. For example, mandatory reporting and limits to withdrawn consent
- How clients can access or amend their personal information
- How clients can make a complaint if they feel their privacy has been breached

Clients' informed consent is to be obtained in writing through the completion of ACSO's 'Release and Obtain Information Form' (ROI). Clients' ROI's are valid whilst ACSO is delivering services to the client, or for a maximum period of 12 months. After 12 months, the completion of a new ROI will be completed.

Where client consent cannot be obtained in writing, For example, telephone based services are provided, informed consent will be obtained verbally and the ECV who collected the consent will complete the ROI over the phone with the client. The ROI's will be stored in the client's case file within their client file.

Clients have the right to withdraw their consent to the collection or use of all or part of their personal information at any time. If a client requests to withdraw their consent, the relevant EVC will:

- Discuss the reasons for the withdrawn and any implications for service delivery with the client. For example, ACSO may be unable to arrange support services for the client.
- Record the withdrawn consent in a case note in the clients file.

Clients also have the right to anonymity by using an alias or not identifying themselves during engagement with ACSO, where it is lawful and practicable.

A unique identifier (combination of letters and/or number) is assigned to client files to identify the client for the purposes of operation. ACSO will not adopt a government assigned individual identifier number e.g. Medicare number as if it were its own identifier.

6.4 Informed Consent - Minor (Children and Young People)

ACSO will protect an individual's personal information in line with this policy regardless of their age. In accordance with the Privacy Act 1988, ACSO does not specify an age after which an individual can make their own privacy decisions. However, a child age under 15 years is presumed to not have capacity to consent. For consent to be valid, an individual must have capacity to consent (APP B.56; Refer to section 6.3 Informed Consent).

Programs where services are delivered to children and young people (Transition to Work; Youth Residential Rehabilitation Services; Problematic Sexualised Behaviour Program and Partners in Wellbeing) will decide on a case by case basis if a client under the age of 18 has the capacity to consent.

As a general rude, a client under the age of 18 has the capacity to consent if they have the maturity to understand the privacy discussion occurring. If they lack maturity, ACSO may determine it is more appropriate for a parent of guardian to consent on their behalf (APP B.57)

In relation to the second paragraph, If it not practical or reasonable for ACSO to assess the capacity of the individuals under the age of 18 on a case by basis, ACSO can presume that a client aged 15 or over has the capacity to consent, unless there is something to suggest something otherwise.

6.5 Dealing with Unsolicited Personal Information

If ACSO receives unsolicited information, it must determine whether it could have collected the information legally (see section 'When personal information may be collected' above).

If ACSO determines that it could not have legally collected that information, then ACSO must destroy the information or de- identify the information as soon as practicable, but only if it is lawful to do so. This does not apply to information in a Commonwealth government record.If ACSO determines that it could have collected the unsolicited personal information, ACSO may retain that information.

7.0 Data Security

ACSO will take reasonable steps to ensure client information will be protected against loss, unauthorised access, use, modification or disclosure.

- ACSO will take reasonable steps to make sure that personal information ACSO holds is accurate, complete, up to date, not misleading and remains relevant to its functions or activities.

- All client records will be kept securely in password-protected electronic client management systems, electronic folders and/or locked filing cabinets, to be accessed only by ACSO personnel with authority to do so. The system has security measures in place that are designed to safeguard the personal information from loss, misuse, unauthorised access and disclosure.

- ACSO personnel are required to ensure that all information held by ACSO remains secure against unauthorised access. This includes personal information about individuals as well as any other information about ACSO's operations that is not already public knowledge. Information about ACSO's commercial agreements and how it performs them must also be kept confidential and protected from unauthorised access or disclosure.

- Client information in paper or electronic form must not be transported out ACSO locations unless authorised and it is necessary to do so (for example, transporting between ACSO locations to Correctional facilities) When necessary, the documents should be transported securely in locked bag or password protected electronic device. Documents must not be left in cars overnight.

- Copies of documentation containing client personal information may only be made if necessary:

    - For an above purpose, and the risks have been considered and mitigated, or

    - To meet legal or contractual requirements. For example, a subpoena

- If ACSO discloses personal information to a third party, reasonable steps must be taken to prevent unauthorised use or disclosure by the third party.

- ACSO does not generally transfer personal information overseas. ACSO may only transfer personal information interstate or overseas if it is permitted to do so under the relevant laws. It will be necessary to comply with the requirements under APP 8 of the Australian Privacy

Principles and the relevant privacy laws in each state affecting by a proposed transfer of information interstate or overseas.

8.0 Clean Desk Policy

To improve the security and confidentiality of data, ACSO has adopted a Clean Desk Policy which all ACSO personnel must comply with, regardless of whether they are working from home or a hub. Maintaining a clean desk reduces the risk of privacy/data breaches in ACSO, as it will decrease the likelihood of internal and external unauthorised access to personal or sensitive information (client, ACSO personnel and ACSO intellectual property).

'Clean desk' refers to how all ACSO personnel are required to maintain their workspace, computer, mobile devices, printed materials and access cards to enhance privacy and information security. This policy establishes requirements for how ACSO personnel should handle personal and sensitive information and materials (client, ACSO personnel and ACSO intellectual property) regardless of their workplace. The policy applies to the use of computers, mobile devices, printed materials, and access cards, as well as for how workspaces should be maintained. To view the guidelines, please read '[Maintaining Privacy and Information Security: 7 practical guidelines for maintaining a clean desk]'.

9.0 Data Retention

ACSO must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose, unless an exception applies. For example:

- The information is in a Commonwealth government file;
- Health service provider files must be retained for at least 7 years after the last health service they provide (and until the individual is at least 25 years old), and ACSO must retain records of the individual's name, the period covered and the deletion date once those files are deleted;
- ACSO must not otherwise delete health information unless permitted or required by law.

For further information on ACSO's management of records, please refer to [IT5 Records Management Policy.]

10.0 Access and Correction of Personal Information

i. Clients have a right to access and correct their personal information held by ACSO. ACSO will provide a client, or their requested representative with access to their personal information upon

request, except in specific circumstances as outlined within the applicable privacy laws. Requests to access client personal information will be actioned and completed within 28 business days of receiving the request.

Where ACSO holds personal information about an client and the client is able to establish that information is incorrect, ACSO must take reasonable steps to correct information as soon as is practicable but within 30 days of the request. When making a correction:

-
    - Record the date and the name of the person making the correction; and
    - If the incorrect information has previously been provided to a third party, notify them of the correction.

ii. If ACSO however denies access or correction to such information, then ACSO will provide the individual with reasons for such decision and advise the individual of mechanisms available to complain about the decision. In the event that ACSO and an individual disagree about the veracity of the personal information held by ACSO, then if requested by the individual, ACSO will take reasonable steps to record a statement relating to the disputed information on the record where the information appears. (Refer to 'Data retention' above in relation to requests to delete information.)

Requests to access or correct client personal information can be forwarded to ACSO's Privacy Officer, via:

Email: privacyofficer@acso.org.au

Mail: Privacy Officer,

1 Hoddle Street,

Richmond, VIC 3121

iii. All clients engaging in ACSO's services will be provided with information about how to make a complaint should they not agree with ACSO's decision to deny access or correction to their personal

information, or they become aware or suspect their privacy has been breached. All complaints, including complaints made on a clients behalf will be responded to according to ACSO's Feedback Management Policy.

iv. An individual may complain about ACSO's handling of personal information. ACSO's complaints resolution processes will endeavour to be fair and equitable. The privacy, confidentiality and dignity of the complainant shall be maintained. All complaints shall be investigated and followed up promptly and courteously by the Complaints Officer with active engagement of the complainant and/or their representative.

Refer to ACSO's Responding to Requests for Personal Information Procedure for further details.

11.0 Privacy Data Breaches

ACSO will manage the process of dealing with actual or suspected data breach in accordance with the national Notifiable Data Breach Procedure which complies with *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

Refer to ACSO's Notifiable Data Breach Procedure for further details.

12.0 Policy Implementation Monitoring

- Privacy Audits

13.0 Other Policies and Procedures to be Cross-referenced with this Policy

- Gp3.1 Responding to Requests for Personal Information Procedure
- Gp3.2 Notifiable data breaches procedure
- CG3 Feedback Management Policy
- G12 Records Management Policy & Framework
- IT7 Information Security Policy

- Standard Operations Procedure

14.0 Cross-reference to Accreditation standards

- QIC Health and Community Services Core Module standard 1.6, 1.7, 2.4
- Human Services Standards, standard 4
- NDIS Practice Standards and Quality Indicators July 2018 in its 8.0 National Disability

15.0 Relevant Legislation

ACSO and McCormack Housing will comply with all relevant Federal and State legislation.

16.0 References

N/A

17.0 Forms related with this Policy

- Gf3.1 ACSO Consent to Release and Obtain Personal Information Form (ROI)
- Gf3.1.2 ACSO Consent to Release and Obtain Personal Information Form (ROI) - Plain English Version
- Gf3.2 Request for Personal Information form
- Privacy policy infographic

18.0 Review

This policy will be reviewed at a minimum of every two years.

Version	Date	Author	Reason	Sections
4.4	19 Nov 2020	Advisor, Q&R	All privacy policies and procedures were reviewed as per the 2 yearly review schedule	All
4.3	14 Sep 2020	Advisor, Q&R	Changed the policy name	Name
4.2	16 Apr 2020	Advisor, Q&R	Clean desk policy included as a gap was identified in a privacy breach assessment	4.1
4.1	30 Aug 2018	Executive team	Approval	All
4.A	08/05/2018	M Q&R	Compliance with *Privacy Amendment (Notifiable Data Breaches) Act 2017*	4.5
4	27/10/2016	HWL Ebsworth Lawyers	Compliance with requirements in NSW and QLD	All
3	26/11/2015	HWL Ebsworth Lawyers	Identified gap	All
2.1	08/04/2014	Leadership	Approval	All
2.B	24/3/2014	QIPO	Include additional information based on Gemba's Self Assessment form	All
2.A	14/03/2014	SMHR	Due for a review & Reflect changes in the Privacy Act	All
2	13/04/2006	DCEO	Reviewed Policy	All
1	05/05/2000	Executive Director	Identified gap	All