

## PRIVACY and CONFIDENTIALITY Policy & Procedure

<b>QA REFERENCE</b>	M't P&P No 16
<b>INTRODUCED</b>	21 <sup>st</sup> July 2008
<b>LAST REVIEWED</b>	18 <sup>th</sup> August 2020
<b>NEXT REVIEWED</b>	18 <sup>th</sup> August 2023
<b>RESPONSIBILITY</b>	The Operational Leadership Group lead by the Manager Performance and Risk is responsible for the review and currency of this policy and procedure document.
<b>APPROVED</b>	Approved by the Chief Executive Officer on 18 <sup>th</sup> August 2020.
<b>ENDORSED</b>	Endorsed by the OLG at a meeting of the committee on 18 <sup>th</sup> August 2020.
<b>RATIFIED</b>	Ratified by the Board of Directors by resolution at a meeting of the Board on 4 <sup>th</sup> November 2020. <i>This policy is valid from the date of introduction and remains in force, as amended from time to time, until such time as formally revoked by resolution of the Board of Directors.</i>
<b>REFERENCES</b>	
<b>Related Legislative Acts and Other Sources of Authority</b>	<ul style="list-style-type: none"> <li>• The Australian Privacy Principles in the Privacy Act 1988 (Cwlth);</li> <li>• The Information Privacy Principles in the Privacy and Data Protection Act 2014 (Vic); and (where personal information is also health information) The Health Privacy Principles in the Health Records Act 2001 (Vic)</li> <li>• Privacy and Personal Information Protection Act 1998 (NSW)</li> <li>• Health Records and Information Privacy Act 2002 (NSW)</li> </ul>
<b>Related Standards, Guidelines and Other References</b>	<ul style="list-style-type: none"> <li>• Performance Standards for Registered Housing Agencies</li> <li>• DHHS Victorian Housing Register Operational Guidelines</li> <li>• Guidelines for Registered Housing Agencies published by DHHS</li> <li>• Commonwealth Ombudsman</li> <li>• Disability Services Commissioner</li> <li>• Human Services Standards</li> <li>• Child Safe Standards</li> <li>• Complaint Handling Guide - upholding the rights of children and young people</li> </ul>
<b>Related MASP Policy and Procedure Documents</b>	<ul style="list-style-type: none"> <li>• Code of Conduct - HRM P&amp;P No 12</li> <li>• Conflict of Interest – HRM P&amp;P No 28</li> <li>• Privacy and Information Security - tenants and prospective tenants - M't P&amp;P No 39</li> <li>• Staff Grievances – HRM P&amp;P No 10</li> <li>• Disciplinary Procedures – HRM P&amp;P No 17</li> </ul>
<b>Related MASP Instructions and Guidelines</b>	<ul style="list-style-type: none"> <li>• MASP Privacy and Confidentiality Brochure</li> <li>• Working Together: You and MASP Brochure</li> </ul>

<b>Related MASP Forms and Templates</b>	<ul style="list-style-type: none"> <li>• Confidentiality Agreement – Employee, Volunteer, Carer, Student – HRM F&amp;T No 53</li> <li>• Information Request – CWG F&amp;T No 44</li> <li>• Authority to Obtain and Release information – M’t F&amp;T No 09</li> </ul>
<b>ACRONYMS/DEFINITIONS</b>	
<ul style="list-style-type: none"> <li>• Privacy Officer</li> <li>• Privacy</li> <li>• Confidentiality</li> <li>• MASP</li> <li>• OLG</li> </ul>	<ul style="list-style-type: none"> <li>• A member of the Operational Leadership Group, appointed by the Chief Executive Officer, currently the Manager, Performance and Risk</li> <li>• In terms of information, privacy is the right of an individual to have some control over how his or her personal information (or personal health information) is collected, used, and/or disclosed.</li> <li>• Confidentiality is the duty to ensure information is kept secret only to the extent possible.</li> <li>• Mallee Accommodation and Support Program Ltd</li> <li>• Operational Leadership Group</li> </ul>

## PURPOSE

To outline MASP’s commitment under privacy laws to ensuring the privacy and confidentiality of all people accessing MASP services and all staff and volunteers involved with MASP.

## SCOPE

The principles in this policy and procedure apply to all information collected, in their work with clients, by and/or disclosed to MASP employees, volunteers, carers and students on placement (in this policy referred to as “staff”). The principles also apply to members of the governing body who occasionally receive client information as part of their governance role.

MASP requires all persons to be maximally protective of client’s rights to confidentiality and privacy consistent with the Australian Privacy Principles as follows.

1. Management of Personal information in an open and transparent manner
2. Allowing client anonymity and pseudonymity
3. Collection of Information
4. Unsolicited personal Information: dealing with
5. Notification to the individual of the collection of personal information
6. Use or disclosure of personal information
7. Use of Information in Direct Marketing
8. Cross border disclosure of personal information
9. Use of Government related “identifiers”
10. Quality of Personal Information
11. Security of Personal Information
12. Access to personal Information
13. Correction of Personal Information

## Responsibility for Implementation and Authorisation of Disclosures without Consent

At MASP, the Privacy Officer takes on the role to educate and assist MASP staff to be aware of and observe the principles and practices laid down in this and related instructions about privacy and confidentiality.

The Manager Performance and Risk is currently the position nominated to perform this role and is the first line of contact for advice about requests for disclosure of client information which do not come with clear written client authority/consent and where staff are uncertain about release/disclosure (e.g. family members seeking information about contact details, police seeking information over the phone, without written request etc.).

Where the case is straight forward and/or clearly requires denial of the request for disclosure, the Manager Performance and Risk will recommend a course of action to the staff member.

Only this Manager and the CEO can make decisions about release of client information where client consent is not forthcoming and handle any subpoenas received. Team Leaders and other Managers do not have authority to permit disclosure of client information without client consent.

## **POLICY**

MASP is committed to protecting and upholding the right to privacy of clients, staff, volunteers, governing body members and representatives of agencies we deal with. In particular MASP is committed to protecting and upholding the rights of MASP clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

MASP requires staff, volunteers and governing body members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

MASP will follow the guidelines of the *Australian Privacy Principles* in its information management practices.

MASP will ensure that

- it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel;
- clients are provided with information about their rights regarding privacy;
- clients and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature;
- all staff, governing body members and volunteers understand what is required in meeting these obligations;
- it will adhere to all requirements imposed under the *Privacy Act 1988*, including the requirements imposed by the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, to strengthen the protection of personal information.

This policy conforms to the *Privacy Act (1988)* and the *Australian Privacy Principles* which govern the collection, use and storage of personal information.

(Note: The Privacy Act applies to organisations with an annual turnover over \$3m or organisations that are health service providers, operators of a residential tenancy database, a contractor that provides services under a Commonwealth contract, an organisation that is related to a larger organisation or one which trades in personal information.

Many funding contracts may require that funded organisations comply with the Australian Privacy Principles).

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

## **PROCEDURES in relation to the Australian Privacy Principles**

There are thirteen Australian Privacy Principles (APPs) and they govern standards, rights and obligations around: the collection, use and disclosure of personal information, an organisation or agency's governance and accountability and the rights of individuals to access their personal information. MASP seeks to be consistent and compliant with the thirteen Australian Privacy Principles.

The following section details the specifics of these principles as they apply in practice at MASP. Where there are variations between stated MASP policy and the Privacy Act, the Privacy Act takes precedence.

- Agencies must have a 'client accessible' Privacy Policy containing details of information collected by MASP and about how to complain about breaches and about incorrect disclosure actions. The Policy must be available free of charge and be available in a suitable form (for the capacities of the client).
- Agencies must actively implement policies and practices to ensure compliance with the APP's.
- As well as allowing client anonymity, agencies must allow use of pseudonyms (within reason).
- Collection of personal information only when reasonably necessary and collection of sensitive information only with the client's consent.
- Collection must come from the individual only (unless the individual consents to information being sought from other parties).
- Unsolicited information, which would not reasonably be collected in accordance with privacy principles must be de-identified or destroyed (if lawful to do so).
- Agencies must make clients aware of personal information being collected and must make them aware of access options, correction options and complaints options.
- Adds new exemptions for disclosure e.g. missing persons, selected legal process purposes, specific dispute resolution.
- Significant restrictions on using client data for direct marketing.
- Restriction on overseas information disclosure.
- Emphasises relevancy of personal information collected (as well as being accurate, up to date and complete).
- Requires organisation to de-identify or destroy personal information it no longer needs for an authorised purpose (unless required by law to keep).
- Stronger imperative to give access within a reasonable period at no cost for making request.
- Making it easier and more 'client friendly' to correct personal information and within a reasonable time.

### **Privacy Principle 1**

#### **Management of personal information in an open and transparent manner**

The way MASP handles the collection, storage and disclosure of personal information must be in accordance with the Australian Privacy Principles (2014) and be transparent and open.

The Privacy and Confidentiality P&P is available to the public and to MASP clients, a summary of the contents of this policy will be conveyed to all clients at initial contact stages.

Avenues for appeal and complaint about MASP practices and policies and tenancy issues and concerns are clearly explained and easily available in MASP's Complaints Management P&P No 01 and MASP's Complaints and Appeals M't P&P No 30 available on the MASP website.

MASP brochure *Privacy and Confidentiality* must be given to the client at the intake interview stage and MASP Privacy and Confidentiality policy clearly explained. This is mandated under the MASP Case Management and Casework Practice Overview - CWG I&G No 05. The brochure is also available in reception at MASP Head Office and at other MASP workplaces.

Generally, MASP staff will explain the following aspects of MASP policy.

- What kind of information is being held, and planned on being collected.
- Why the information is collected, (for lawful purpose to provide them with best service from MASP).
- How the information is collected.
- MASP policy regarding client consent to disclosure of information both within MASP and to external agencies / bodies.
- Who outside MASP, would we seek consent for information to be released to or shared with (including overseas disclosure).
- Consequences (if any) of the client withholding information required (as is their right).
- Who at MASP will be storing and using the information (those MASP staff who have a need to know, including supervisors). The client should also be made aware that the information may be shared for internal reviews and analysis.
- Legal obligations of MASP to provide progress details to certain authorities (particularly when the referral (attendance) to MASP was statutory/compulsory).
- How the client can access / see their information.
- The limitations to confidentiality (e.g. in relation to legal processes where information is required by subpoena or when client's life or other person's life is at risk).
- How the client can request corrections to personal information held.

There may be exceptions to these requirements where the client is not able to comprehend due to mental, intellectual or physical impairment or disability. In all cases however, attempts should be made to give optimum information to the extent of the client's ability to absorb, by whatever means are available (e.g. pictorial tools etc.) AND to ensure that advocates or parents/guardians are made aware on the client's behalf.

MASP will take reasonable steps to make its Privacy & Confidentiality Policy available in a variety of forms to meet the needs of clients including hard and electronic copies.

#### Limitations: Harm and Criminality

Clients should be aware that although MASP staff have the highest standards in relation to the privacy and confidentiality of personal information given to them, that they also have a duty to report information conveyed to them that indicates significant criminal activity or likelihood of the client harming self or others. i.e. that MASP do not have a legally privileged position or requirement in relation to maintaining confidentiality in these cases.

## **Privacy Principle 2**

### **Allowing client Anonymity and Pseudonymity**

Individuals, particularly voluntary clients seeking service have the option to not identify themselves or to use a pseudonym and to withhold certain information.

If the client refuses to give certain information, MASP should still provide service within the boundaries of the information they do have.

It should be explained to the client how the lack of information could affect MASP's ability and capacity to provide service but MASP's staff can work within the limitations. A client has a right to remain anonymous.

This principle will not apply fully to clients who are under a court / tribunal order to attend MASP or who are statutory clients of government departments and referred to MASP.

---

## **Privacy Principle 3**

### **Collection of Information**

This principle seeks to put limitations on what is collected and sets basic quality standards.

**Only collect that which is necessary and relevant.** MASP always needs to collect a minimum amount of personal and sometimes sensitive information from clients (to enable it to deliver the service or program sought by clients or required to be delivered by a referring statutory agency.)

As with all information collection, the information collected must be relevant to the service being provided and only information that is needed should be collected. 'Needed' information is that which is reasonably necessary to make decisions about service delivery.

#### **Sensitive Information**

There are specific restrictions on collection of 'sensitive' information which includes religious beliefs, political opinions, memberships of organisations, sexual preferences, history or orientation, criminal records, racial or ethnic/cultural origin or information of a similar kind. It also includes health information and certain genetic and biometric information.

Generally, this is intensively personal information or history which will rarely be relevant to the provision of the MASP service being offered. Where it is collected at MASP it mainly focuses on cultural background and is collected to ensure client needs are properly understood and to enable MASP to provide the most appropriate services.

At MASP we are required to ensure people from CALD and ATSI backgrounds get the same high standard of service as any other client and thus we are required to explain this to the client before asking questions about their CALD /ATSI backgrounds in order to better assist them. Clients have the right not to supply this information to MASP.

MASP staff should be very careful when collecting the above categories of information and be very clear in why they are doing so. If done as a requirement of MASP to provide a better service, by a funding body or by law they should explain such to the client. The client's permission must be obtained when collecting sensitive information.

**Information should be factual and correct**

Staff should be careful about the quality of the information they collect and take care that it is factual, correct and current. In the first instance staff should check with the client about information received from other agencies or referral sources. Over time the currency of other information should be checked.

**Collected from client**

Information should be collected in a lawful and fair manner with the knowledge of the client. Information collecting should be a non-intrusive and transparent process and should be collected only directly from the individual or their nominated representative. Clients should be made aware of their right not to give information.

**Collected via referral process**

Other information available to MASP but not collected by them e.g. conveyed by a referring body at referral stage, for instance, should be discussed with the client so they are aware of MASP's information holding on them. (Note that such information sent from another agency would usually be subject to the referring agency's own privacy policy and would usually have required client consent for its transmission to MASP.)

There may also be some cases where compliance to the requirement above, (explaining specific information held) would prejudice the health, safety and welfare of the individual or community. In these cases discussion with the Privacy Officer is required to agree on boundaries.

The individual must be made aware of a range of considerations in respect of their information as set out below.

---

**Privacy Principle 4****Dealing with unsolicited personal information**

Other information such as newspaper cuttings about the client, unsolicited reports etc. should not be collected by MASP staff or held on file under any circumstance. (We do not build up "dossiers" on MASP clients).

Where unsolicited information is received by MASP it should be assessed as to whether it meets the test in APP3. e.g. is it relevant, factual and current and the sort of information that MASP would normally collect?

If it is deemed not to meet the above test the information should be destroyed or de- identified. If the identity of the provider is known the information should be returned to them.

---

**Privacy Principle 5****Notification to the individual of the collection of personal information**

Generally, staff should always keep the client well informed of the purpose of the collection of any personal information and which relevant Australian law, court or tribunal process authorises information collection, transmission or disclosure.

The staff member should explain why MASP seeks to collect the specific information, the service limitations /consequences if certain information is not collected and who personal information is proposed to be transmitted to both internally and externally.

Part of the notification process should be the giving of information about MASP Complaints Management process. (In relation to instances of lack of compliance to the APPs).

If MASP staff receive external referral information and are unsure whether the client knows about the specifics of the information, it is particularly important for MASP staff to advise the client about what entity sent the information and what information was received.

---

## **Privacy Principle 6**

### **Use or disclosure of personal information**

Clients may give MASP consent to release information to third parties (individuals or organisations).

The general rule is that no information may be released to these individuals or organisations **without the client's consent in writing.**

This written authority can be obtained in a number of ways but most commonly it is

- via the **Authority to Obtain and Release information** CWG F&T No 09 which is normally completed during the initial contact stage;
- from specific authorities developed especially for the purpose;
- from the standard authority forms of other agencies.

Such authorities need to be carefully perused and kept on the client file on Prosims and a file note made about any information disclosed which has been previously authorised.

Such consent for disclosure must be informed, freely given, specific and current.

Informed means that the client is fully aware about who is seeking the information, what information is being shared, for what purposes it is being sought and what the consequences of releasing the information are.

In general, clients should be encouraged to let MASP share their personal information with other human service and/or health agencies where such sharing will help get a service or benefit that is being sought by the client.

MASP believe that sharing information can promote coordination and continuity and can absolve the client in not having to repeat the same information time after time. Sharing promotes better and faster access to a range of services, provided it is with the client's permission.

Freely Given means that clients will not be coerced into disclosing information. If, after explaining the reasons for disclosure, a client wishes not to disclose, this is their right. (However, if there are negative consequences of not disclosing these must be explained)

Specific means that only specific information relevant to the specific request will be disclosed. It is not necessary to disclose/share all information held – only that which is relevant.

Current means that the information to be disclosed relates to the current episode of service at the present time.



Should information change and a further request based on an older authority be received, a new authority would need to be prepared. In general, information about the client held by MASP should be continually checked for currency, accuracy and completeness.

In all of the above, open discussion with the client is required before they are asked to let MASP disclose information to other parties. Information disclosure is a serious business.

MASP staff must aim to ensure that what is disclosed by MASP is clearly sanctioned by the client (or is relevant to serious 'duty of care' considerations when not sanctioned or where permission is not sought).

### **Other MASP staff**

There are occasions when both personal and health information needs to be shared between staff or with carers at MASP. There is an understanding that privacy provisions allow sharing of key information within the agency.

However, not all information gained need be shared. Only that which is essential in providing good care. In all cases staff who have the information need to ask - does the carer/worker need to have the information? Do they need to know this information in relation to their role and responsibility?

Without this information being shared, is there a risk of harm to the client OR to the workers?

MASP staff need to balance MASP commitment to privacy with MASP duty of care to carers and staff (particularly their safety) and MASP need to provide good care.

### **Spouses, Family and Friends**

These individuals must be advised that we are prohibited by law from unilaterally disclosing any aspect of the client's situation, even to advise whether the client is a client or has attended the agency.

### **Human Service Organisations**

Essentially, most human services organisations are fully aware of the principles of the legislation regarding privacy and confidentiality and will always support requests for information held by MASP with signed consent forms from the client.

Where agencies/authorities submit specific requests for information disclosure they should be asked to include in the request an indication of why the information is being required and what it will be used for.

### **Funding Bodies**

From time to time, funding bodies, e.g. DHHS, FACS will require access to client information in relation to their progress /outcomes etc. for purpose of audit, evaluation and/or review or to assess MASP competence in respect of accreditation/registration standards. This information can be released and access can be given to external reviewers to MASP client files, provided the CEO is satisfied of its bona fides.

In all cases the CEO should be informed that disclosure is being required. The written request by the funding body/external reviewer should be identified.

The Privacy Officer will supervise access and disclosure in these cases.

If possible and acceptable for the purpose for which the information is required, it could be given 'de-identified', (names removed etc.). MASP will always seek the least disclosure that will fulfil the purpose of the request.

## **Police**

Police should be asked to produce a written request such as a warrant for the information sought. Under no circumstances is information to be released just to help police contact a client. (Although there are now exceptions which allow disclosure where missing persons are involved).

## **Legal professionals**

Information is not to be provided unless a subpoena has been provided.

Staff should consider such requests carefully and not be pressured to respond hastily. Always check disclosure request situations with the Privacy Officer or supervisors. The Privacy Officer (or CEO in the absence of the Privacy Officer) is the final authority on such cases.

## **Disclosure of Client Information to the Staff member's Spouse and Friends**

The prohibition regarding disclosure of client information applies not only in respect of work and professional relationships but also in respect of private and social relationships. This is even more so in small towns where general client circumstances can easily be recognised and related to specific individuals.

Staff are prohibited from discussing client casework /client details in any way outside the work environment in any form that could remotely be identified to any particular individual.

It is totally unacceptable to be disclosing client names (as a client of the XYZ service) or client history or current details to any other person, spouses included.

General client discussion, even without specific identifying detail, in social scenes is also very unacceptable. It does the image of the agency no good whatever when casework staff are seen to be discussing client idiosyncrasies in an "after work" social setting. It also makes those individuals who overhear the discussion and who may become clients of other services very wary of the care and 'confidentiality' of the community service sector.

Finally, staff should be careful in not discussing client matters (even when no names are mentioned) in public areas such as reception areas, publicly used toilets, waiting areas, offices with doors open etc., where they can be overheard.

## **Information Disclosure in the Health and Safety Interests of the Client or Third Parties (Duty of Care)**

Sometimes information needs to be disclosed, either unilaterally or in response to a request, without any consent or without the client's knowledge in order to fulfil MASP commitment to Duty of Care.

Such disclosure decisions are very serious and should have the approval of the Privacy Officer or CEO.

Guidelines for disclosure without consent revolve around safety and include situations

- where the health or safety of the individual or another related /dependent party is compromised or could be compromised;
- where the safety of other persons is at risk;
- where the safety of staff is at risk;
- where the safety of the workplace is at risk.

It is impossible to detail all situations but the following are very indicative

- Where the client issues substantial threats of violence or harm in respect of him/herself or others.
- Where there is evidence or indication of actual self-harm to self or significant others (children etc.) e.g. overdoses / assault marks.
- There is reason to believe serious unlawful behaviour has been entered into or contemplated /planned.
- There is abuse of others or neglect of others, particularly dependents.
- Where medical/emergency treatment needs to be given.

If the staff member, volunteer or governing body member believes a client's life is at risk and are required to call for emergency support/assistance (e.g. ambulance, police) they may disclose relevant personal or health information to the emergency services.

In an emergency, disclosure of whatever is reasonable, is acceptable particularly when the disclosure serves to protect a person from an imminent threat to their life. It is not reasonable to wait to get consent to release information to an ambulance or medical practitioner from parents/guardian etc.

As with all requests, staff need to be wary of telephone contact from people claiming that they are a hospital or other medical/allied health professional (or police and lawyers for that matter) and seeking personal information. Ask for identification and name and contact number of institution and ring the Institution back. If in any doubt the staff member should involve their supervisor or a member of the OLG.

Privacy and Confidentiality principles are always secondary to Duty of Care considerations where the immediate health or safety of the client or others is seriously or could be seriously compromised.

All such disclosures should be documented thoroughly, clearly stating the reasons for the disclosure and the internal approval process utilised.

### **Seeking Consent by Third Parties on Behalf of the client: Emergency**

There may be times when consent is needed urgently to release information but the client cannot or will not give consent. This is often in emergency situations.

In MASP's initial information collection activity with clients we have identified carers or guardians, particularly those who have legal guardianship or power of attorney roles in respect of a client. This should always be identified for clients with intellectual or other disabilities.

In case of emergency, where the client's life is at risk with an immediate threat to their life, safety or welfare and the client cannot or will not give consent, then the client's guardian etc. should be contacted. If they cannot be contacted quickly or the emergency situation requires immediate response, the caseworker (in consultation with a supervisor) can disclose personal or health information and do whatever they think the guardian would expect them to do without their consent. In this situation, whatever is reasonable as a duty of care is an acceptable disclosure.

Some general points to consider in response to unauthorised disclosure

- Is the situation life threatening and/or a significant risk to safety or welfare?
- Is it in the best interests of the client?
- Is it legal to do so?

- Is there a risk that sharing/disclosing may cause negative consequences for another person e.g parent or family member (outweighing the risk to the client)?.

Some decisions are very difficult to make and when weighing up the pros and cons. Workers should always consult with senior workers before making unauthorised disclosures unless the matter is a life-threatening emergency as above.

---

### **Privacy Principle 7**

#### **Use of Information in Direct Marketing**

MASP policy is not to release information outside MASP for the purposes of direct marketing or advertising. Where a service which wishes to contact MASP clients is judged by MASP (by a Program Manager) to provide a potentially useful service, MASP may contact the client to ask them if they wish their (specific) contact details to be released to the specific marketer. The contact details of positive response clients (consent given in writing only) may then be disclosed to the marketer.

Although MASP does not want to become a post box function for the public there are some simple steps staff can take when passing on information which is deemed to be beneficial to the client.

To do so, without breaching disclosure rules, the MASP caseworker to make contact with the client to let them know of the approach, give them the third-party contact details and ask them to make contact with the parties seeking to make contact if they so desire.

Alternatively, the case manager may forward on written information to the client under cover of an explanatory note.

---

### **Privacy Principle 8**

#### **Cross border disclosure of personal information**

Because of the proximity of services in NSW and South Australia, MASP may allow disclosure to services in those states, provided all other conditions in PP 6 are followed (particularly client consent).

MASP does not disclose information to any entity in other countries without express and explicit written permission of the client.

---

### **Privacy Principle 9**

#### **Use of Government related identifiers**

MASP staff are not to use government identifiers as part of their own identification methods e.g. Tax File Numbers, Medibank numbers etc.

---

### **Privacy Principle 10**

#### **Quality of Personal Information**

MASP staff must take reasonable steps to ensure that information that they collect is:

**Freely Given** - means that clients will not be coerced into disclosing information. If, after explaining the reasons for seeking information, a client wishes not to disclose, this is their right. (However, if there are negative consequences of not disclosing, these must be explained).

**Specific** - means that only specific information relevant to the specific request for service will be collected.

**Current** - means that the information collected relates to the current episode of service at the present time. Should client information change and a further request for disclosure of information based on an older consent authority be received, a new authority would need to be prepared. In general information about the client held by MASP should be continually checked for currency, accuracy and completeness.

---

## **Privacy Principle 11**

### **Security of Personal Information**

Information about clients is documented on various MASP forms, MASP templates and pro-formas and on other forms required by funding bodies. These is often stored on hardcopy paper files. MASP also collects and stores data on client data bases required by statutory funding bodies such as DHHS & FACS (eg IRIS, CRIS/CRISSP, SMART etc).

General rules for data we store are as follows.

- Files and individual forms etc. must be stored securely and not in view (or potentially in view) of anyone other than MASP staff.
- At all times files on desks in public view, must be covered so as not to show client names.
- Every night any client files should be securely locked away in lockable and locked file cabinets.
- Photocopying and faxing (transmission and receipt) must not be viewable by anyone other than MASP staff.
- Archived files must be secured in an area inaccessible to anyone other than MASP staff.
- Client information **stored** on computer can only be stored in password protected computers and client data must never be transferred by internet/email unless encrypted.
- Where client names are written on the front cover of files, staff must be particularly mindful and vigilant of keeping the cover from being seen by other individuals.

### **Transmitting Client Information**

Staff must take extreme care when **transmitting** client information by each of the following means

#### **Fax**

The fax operator to be highly vigilant and to take utmost care in transmitting the document to the correct fax number.

#### **Post**

The information must be sent by registered or certified mail, marked personal and confidential, to the person receiving it.

#### **Computer**

Preferably to be sent by encrypted transmission, this would almost always be via a recognised information transfer arrangement such as with Connecting Care.com. The alternative is to send emails that are password protected.

## **Privacy Principle 12**

### **Access to Personal Information**

Clients are allowed access to their personal information and have a right to view their personal file, however, if there is information on this file about any other MASP client or confidential or sensitive information about, or from, people known to the client, parts of the file may be withheld.

The Privacy Officer handles all requests for formal viewing of the file. Clients will complete the form - Information Request - CWG F&T No 34.

Reports from third party professionals can be given to the client provided that there is no information that has been identified by the professional as “not to be released” or no information about any other client in the report.

Requests for personal file access from clients should be given to the Privacy Officer who will inspect the file and remove (or omit copying) such information as detailed in the paras above.

Clients will be allowed to read their file at MASP but not to remove them from the building. Where copies of individual information/reports are required, the Privacy Officer can photocopy it for the client, subject to exceptions as identified immediately above.

Clients wishing to access their personal file should make contact with the Privacy Officer or case worker (who will contact the Privacy Officer). There is no cost for access.

If case managers are transparent about information held and clearly explain MASP’s privacy policy, it is not expected that there would be a significant number of clients wishing to view files.

---

## **Privacy Principle 13**

### **Correction of Personal Information**

The client has a right to seek corrections or additions to update or make complete the information to their file.

MASP must ensure that information it holds on file is accurate, current, complete, relevant and not misleading for the purpose for which it is held.

Staff should take reasonable steps to achieve this result. Where clients request correction action on their information and MASP believe the information held or stored is incorrect, the correction should be taken.

Clients must put their request in writing stating what information is incorrect (there is no specific form). However, where it is clear that wrong information is stored by mistake or incorrect transcription, such written formalities will not be necessary (but a brief note in file notes would be appropriate).

Other agencies to whom information has been given should be advised of the agreed correction in writing.

Where MASP do not believe correction is necessary the Privacy Officer must advise the client in writing of

- the reasons for the refusal

- the mechanisms for a **formal complaint** about the refusal to correct.

MASP has 10 days maximum to respond to a request for correction.

---

### **MASP staff ceasing employment**

MASP staff should be prohibited from disclosure of client information by action taken at the start of their employment at MASP.

When employees join the organisation, they would have been asked to sign a confidentiality agreement clearly prohibiting disclosure of client information at any time whether as an employee or not.

They should be reminded of this agreement when they cease MASP employment.

Staff should be reminded that the unreasonable and/or unjust disclosure of personal and private client information without the client's permission could become the subject of a civil claim.

---

### **Documenting Disclosures**

Where a disclosure is made (for whatever reason) it must be recorded on the client file stating reasons for the disclosure and the action taken. The worker involved and their supervisor must sign the record.

---

END DOCUMENT

---