POLICY DOCUMENT

Privacy

Document name:	Privacy 1019.5
Management Committee approval date:	6/10/2023
Review period:	3 years
Review date:	5/10/2026

Policy context: This policy relates to:	
Human Service Quality Framework	**Standard 1 - Governance and Management** *Indicator 7:* The organisation has effective information management systems that maintain appropriate controls of privacy and confidentiality for stakeholders.
Other standards	
Legislation or other requirements	*Human Rights Act 2019* *Information Privacy Act 2009 (Qld)* *Information Privacy Principles* *Right to Information Act 2009 (Qld)* *Privacy Act 1988 (Cth)* *Australian Privacy Principles* *Privacy Amendment (Notifiable Data Breaches) Act 2017* *Notifiable data breaches - Home (oaic.gov.au)* *Information Privacy Act 2009: Obligations of Contracted Service Providers (Office of Information Commissioner Queensland)* *Information Privacy Guide (Department of Children, Youth Justice and Multicultural Affairs)* *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*

1. Purpose: Why do we have a privacy policy?

To provide an effective and high-quality service and to maintain appropriate accountability, we must collect, store and sometimes share relevant personal information about our clients. It is important that we are consistent and careful in the way we manage what is written and said about a client and how we decide who can see or hear this information.

Our clients have legislated rights to privacy. It is essential that we protect and uphold these rights, and also that we act correctly in those circumstances where the right to privacy may be overridden by other considerations.

To uphold the rights of clients to privacy, each staff and management member needs an appropriate level of understanding about how we meet our legal obligations.

2. Scope

This policy will apply to all clients, stakeholders, volunteers and staff of the Mareeba Community Centre Inc.

3. Policy statement: Our commitment

Mareeba Community Centre Inc. is committed to protecting and upholding the rights of our staff, volunteers and clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them. We want all stakeholders to have confidence that we take these responsibilities seriously.

Specifically, we will:

- meet legal and ethical obligations as employees, volunteers and managers in relation to protecting the privacy of clients
- provide clients with information about their rights regarding privacy
- ensure privacy for clients when they are being interviewed or discussing matters of a personal or sensitive nature with staff.

4. Procedures

4.1 Privacy

We manage our obligations in relation to protecting the privacy of our clients by making sure that we meet the requirements of the federal Privacy Act 1988 and the Information Privacy Act 2009 (Qld).

In protecting the privacy of our clients, we ensure they are well informed about their rights and that we take our responsibilities seriously.

In particular, we pay attention to the physical layout of our premises in regard to privacy. We make provision for private interview space when interviewing clients or talking with them about matters of a sensitive or personal nature. We offer home visits or the opportunity to make an appointment outside of opening hours.

4.2 Collection of information

Mareeba Community Centre will only collect what personal information is necessary to provide a service to that individual. Personal information will be collected only from the individual whose information it is, or from their guardian or carer.

4.3 Disclosure of information

Personal information will not be disclosed to people outside Mareeba Community Centre unless:

- the individual explicitly consents to the disclosure or
- the disclosure is required by law or
- a worker believes, with the agreement of another worker or the Manager, that disclosure is necessary to prevent or lessen a serious and imminent threat to an individual or to the public.

4.4 Breach of privacy

Mareeba Community Centre is committed to ensuring it complies with its obligations under the federal Privacy Act 1988 and the Information Privacy Act 2009 (Qld). At all times Mareeba Community Centre will take reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles.

Mareeba Community Centre requires all employees to read and comply with the Privacy and Confidentiality Agreement. In addition, the Privacy Policy is referred to in all Letters of Offer and the Employee Handbook. Strict disciplinary action will be taken should any staff member be found to be breaching client confidentiality and the requirements of the Privacy and Confidentiality Agreement.

Any breach of privacy will be dealt with via the performance management process, as detailed in Policy 6005 Employee Performance and Support, and may result in dismissal.

A data breach, or breach of privacy, happens when personal information is accessed or disclosed without authorisation or is lost.

Examples of potential breaches of privacy include:

- lost or stolen laptops, portable storage devices, or physical files containing personal information
- an agency mistakenly providing personal information to the wrong person
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the organisation; or
- employees accessing personal information outside the requirements of their employment.

The Manager and / or Management Committee is required to notify all Queensland Government funding bodies of breaches of privacy, as stipulated in Section 18.4 of the Queensland Government's Service Agreement – Standard Terms (Version 1.1, dated 17 February 2015).

The Manager and / or Management Committee will also notify the individual / individuals whose privacy has been breached. These individuals will be notified in writing of all steps taken in response to the breach of privacy and will be provided with information as to actions they can take if they do not feel that the situation has been managed appropriately.

4.5 Notifiable Data Breaches

Under the Privacy Act 1988 Mareeba Community Centre must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach involving personal information is likely to result in serious harm.

An organisation must notify under the NDB Scheme if it experiences (or has reasonable grounds to believe that it has experienced) a data breach in which:

- there is unauthorised access, unauthorised disclosure, or loss of personal information,
- the data breach is likely to result in serious harm to one or more individuals affected, and
- the organisation has not been able to prevent the likely risk of serious harm with remedial action.

Serious harm could include:

- physical harm
- psychological harm
- emotional harm
- financial harm and
- reputational harm.

When notifying individuals affected, Mareeba Community Centre will prepare a notification statement which contains:

- the organisation's name and contact details
- a description of the data breach
- the kinds of information involved
- recommendations about the steps individuals should take in response to the data breach.

The OAIC will be notified of the data breach by the submission of the online Notifiable Data Breach form found at: https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB. The notification statement referred to above will be attached to the form.

The diagram on the next page summarises the data breach response process as prescribed by the OAIC. The parts of this process that are required by the NDB Scheme are coloured red.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

4.6 Cyber Security

Mareeba Community Centre collects and stores information and uses various technologies throughout our daily operations. As a result the organisation may encounter cyber risks.

Cyber security is the practice of protecting this information, the organisation's electronic systems and digital information, reducing the likelihood of a breach.

These include:

- internal risks – which originate from within the organisation, and
- external risks – which are the more commonly known risks and are posed by third party hackers.

These risks can result in damage to reputation, identity theft, financial scamming, unauthorised access to mailboxes and network, damage/disruption to systems, data theft and possible breaches of privacy law implications.

As an organisation, Mareeba Community Centre, addresses internal risks through ongoing staff training and awareness and password protection. External risks are addressed using protection and detection software, as well as two factor authentications.

5. Other related policies and procedures

Documents related to this policy	
Related policies	1008 Information Management 1020 Confidentiality 4001 Client Records 4003 Access to Confidential Information 6005 Employee Performance and Support 6010 Acceptable Use of Digital Technology & the Internet
Forms or other organisational documents	Client Privacy and Confidentiality Agreement Staff Privacy and Confidentiality Agreement Client Service Charter Employee Handbook

6. Review processes

Policy review frequency: Every three years	*Responsibility for review:* Manager
Review process: The policy will undergo a review process using the Power Apps system, which automates review reminders and streamlines the approval process. The Manager will review the policy in consultation with other service providers, clients, staff, volunteers, and the Management Committee. Any recommended changes will be tabled for Management Committee approval.	
Documentation and communication: Approved policies are stored in the SharePoint library and accessible for all staff. Staff will be informed of and required to review all changes as they occur.	

Record of Policy Revisions:

Version 1019.1 (adopted 11th January 2017) – added section 4.4 regarding procedures to be undertaken for breaches of privacy.

Version 1019.2 (adopted 29th August 2017)

Version 1019.3 (adopted 19th August 2020) – expanded on section 4.4 regarding breaches of privacy, added Section 4.5 regarding Notifiable Data Breaches Scheme and Section 4.6 Cyber Security. Added reference to further legislation and updated links.

Version 1019.4 (adopted 23rd May 2022) – updated terminology in *section 4.4 Breaches of privacy.*

Version 1019.5 (adopted 5th October 2023) – Added further legislation to first table and transferred policy to new template.