1 Privacy Policy

1.1 Introduction

MDQ is committed to protecting the privacy, dignity and confidentiality of people who engage with its services, including participants, families, carers, donors, staff, volunteers and other stakeholders.

MDQ recognises that personal and sensitive information, including health and financial information, requires careful and respectful handling. Privacy is fundamental to safe, person-centred service delivery, ethical fundraising practice and maintaining trust across all interactions.

This commitment is informed by relevant legislative and regulatory frameworks, including the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and MDQ's broader Quality Framework.

1.2 Purpose & Scope

This policy outlines MDQ's approach to the collection, use, storage and sharing of personal information across service delivery, fundraising and organisational activities.

The policy applies to all MDQ services and to all individuals involved in delivering or supporting those services, including staff, volunteers, contractors and others who have access to personal information.

It provides a framework for:

- managing personal information in a lawful, transparent and respectful manner
- supporting individuals to understand and exercise their privacy rights
- ensuring information is used appropriately to support service delivery, organisational functions and fundraising activities

This policy forms part of MDQ's Quality Framework and is applied in conjunction with related policies addressing safeguarding, service delivery, communication, fundraising and information management.

1.3 Definitions

- **Personal information**: Information or an opinion that identifies, or could reasonably identify, an individual.
- **Sensitive information**: Personal information that includes health, disability, cultural or other protected information requiring a higher level of protection.
- **Consent**: Permission provided explicitly or implicitly for MDQ to collect, use or share personal information.
- **Donor information**: Personal and financial information collected in the context of fundraising and supporter engagement.

1.4 Policy Statement

MDQ respects the right of individuals to privacy and is committed to handling personal information in a way that is lawful, transparent and consistent with dignity, safety and choice.

Personal information is collected, used and shared only where necessary to support service delivery, organisational functions or legal obligations. Information is handled with care, and access is limited to those who require it to perform their role.

MDQ supports individuals to understand how their information is used and to make informed decisions about consent, including how information is shared across services and with external providers. Where participants engage with multiple services, information sharing is guided by consent, purpose and privacy requirements.

MDQ maintains systems and processes to protect personal information from misuse, unauthorised access or disclosure. This includes secure storage, role-based access and ongoing review of information management practices.

Where concerns arise, including potential data breaches or inappropriate use of information, MDQ responds promptly and in accordance with legislative and regulatory obligations.

Through these commitments, MDQ ensures that privacy is embedded in service delivery and supports safe, respectful and person-centred practice.

1.5 Functions & Delegations

Position	Task / Delegation
Board	**Chairperson & Directors** • Governance oversight of MDQ's privacy obligations, ensuring systems are in place to protect personal, sensitive and financial information. • Approves this policy and monitors organisational risk and compliance.
Management	**CEO** • Ensures organisational systems, processes and culture support effective privacy management across service delivery and fundraising. • Acts as an escalation point for significant privacy concerns or data breaches.
Managers (as delegated by the CEO)	**Senior Leaders** • Ensure this policy is implemented within their areas, including staff training, supervision and support. • Provide guidance on complex privacy, consent or information-sharing matters.
Staff	**All Staff & Volunteers** • Manage personal information appropriately in day-to-day practice, including collecting, using and storing information with care, maintaining confidentiality and respecting consent. Identify and report privacy concerns or breaches in line with MDQ processes.
External Stakeholders	**Clients & Donors** • Are supported to understand their privacy rights, make informed choices about how their information is used, and raise concerns or request access or correction where required.

1.6 Procedures

1.6.1 Collection of Information

MDQ collects personal information that is necessary to:

- deliver services and supports
- communicate effectively with participants and stakeholders
- conduct fundraising and organisational activities
- meet legal, regulatory and funding requirements

Where practicable, information is collected directly from the individual and with their consent.

1.6.2 Consent

MDQ obtains consent to collect, use and share personal information through a range of methods, depending on the context and nature of the information. Consent is typically captured through:

- service intake and registration forms;
- digital forms and systems used for service delivery or fundraising; and
- documented records within client or donor management systems.

While verbal consent may be accepted in some situations, MDQ prioritises recorded or written consent wherever practicable.

In fundraising contexts, consent is explicitly sought for communications, and donor preferences regarding contact methods and frequency are recorded and respected. Individuals may update or withdraw their consent at any time.

1.6.3 Use and Disclosure of Information

Personal information is:

- used only for its intended purpose;
- shared only where relevant and appropriate; and
- disclosed with consent or where required by law.

Information may be shared to:

- support coordinated service delivery;
- engage with other providers or professionals (with consent); or
- meet legal or regulatory obligations.

MDQ primarily shares information through secure systems and approved communication methods. Email may be used where appropriate, with care taken to ensure accuracy of recipients and content.

Where information is shared, staff take reasonable steps to:

- limit information to what is necessary for the purpose;
- ensure accuracy and completeness; and
- maintain confidentiality and privacy requirements.

MDQ selects systems and service providers that support appropriate data security standards, including storage of information within Australia or jurisdictions with comparable privacy protections.

When engaging in fundraising or donor communications, MDQ:

- respects requests to opt out or limit contact;
- records and honours donor communication preferences; and
- ensures communication is appropriate, respectful and non-intrusive.

1.6.4 Donor & other supporter information

MDQ collects and manages personal information from donors and supporters to support fundraising, communication and organisational sustainability.

Donor information is:

- managed in accordance with privacy legislation and the FIA Code of Conduct;
- protected through appropriate security measures; and
- used in a manner that respects privacy, dignity and trust.

Donor preferences are actively recorded and managed, including communication methods, frequency and opt-out requests. Systems are used to ensure individuals are not contacted where they have requested no further communication.

Fundraising activities, including phone-based engagement, are conducted in a way that is respectful, transparent and responsive to individual preferences.

1.6.5 Separation of Service Information

MDQ recognises that personal information collected through service delivery, fundraising and finance functions differs in purpose and sensitivity, and requires appropriate separation.

MDQ maintains separate systems for different functions, including:

- client information within the Echidna client database which includes the ability to separate information related to specific services to teams/functions e.g. social work notes not accessible by all client services team members;
- donor and supporter information within the VegaWorks donor database; and
- financial and payment information within MYOB and HRIS systems (including Tanda).

These systems operate independently, with access restricted based on role and function.

Where information needs to be shared between systems or functions, this is undertaken on a limited and purposeful basis. Any manual transfer, import or export of information is managed carefully to minimise risk, ensure accuracy and maintain privacy and consent requirements.

These arrangements support role clarity, reduce the risk of inappropriate access, and ensure personal information is used only for its intended purpose.

1.6.6 Storage and Security

MDQ maintains secure systems and controls to protect personal, sensitive and financial information.

Information is stored within dedicated systems appropriate to its purpose, including service delivery, fundraising and financial platforms. Access to these systems is restricted based on role, team and organisational function.

Access controls include:

- role-based and seniority-based permissions;
- separation of access between service delivery, fundraising and finance functions;
- additional restrictions within service delivery systems (for example, limiting access between different service areas unless appropriate consent is provided); and
- limiting access to information on a “need to know” basis.

Fundraising staff do not have access to client service information, except where individuals have provided consent (for example, involvement in fundraising activities or stories).

These controls support confidentiality, reduce the risk of inappropriate access, and ensure personal information is used only for its intended purpose.

1.6.7 Payment Information and Security

MDQ takes appropriate steps to protect financial and payment information.

Where payments are collected, including over the phone, information is entered directly into secure, compliant payment systems. Payment details are not recorded in MDQ systems and are managed through third-party providers that meet industry security standards.

MDQ uses secure payment gateways and tokenisation processes to protect financial data. Staff do not retain or store credit card details, and safeguards are in place to minimise the risk of unauthorised access or disclosure.

1.6.8 Access and Correction

Individuals may request:

- access to their personal information;
- correction of inaccurate or incomplete information

MDQ supports these requests in a reasonable and timely manner, subject to legal and privacy considerations.

1.6.9 Retention and Disposal

Personal information is:

- retained in accordance with legislative and organisational requirements; and
- securely destroyed or de-identified when no longer required.

Retention practices consider legal obligations, service requirements and the best interests of individuals.

1.6.10 Data Breaches

MDQ responds promptly to actual or suspected data breaches to minimise potential harm and meet its legal obligations. All staff are required to report suspected or confirmed privacy breaches as soon as possible. This may occur through incident reporting systems, direct communication with managers, or escalation to the Privacy Officer.

Data breaches are managed in accordance with MDQ’s Data Breach Response Plan and involve:

- containing the breach and limiting further exposure;
- assessing the nature and impact of the breach;

- determining whether notification is required; and
- reviewing the incident to strengthen systems and practices.

The Privacy Officer provides oversight of data breach management, including assessment, escalation and external notification where required. Timely reporting is critical, and early response is prioritised to reduce risk and potential harm.

1.6.11 Recognising a Privacy Breach

A privacy breach occurs where personal information is lost, accessed, disclosed, or used without authorisation. Examples may include:

- sending information to the wrong recipient;
- sharing more information than is necessary;
- accessing information without a clear purpose; or
- losing devices or records containing personal information.

Staff are expected to take a proactive approach to identifying potential breaches and to report concerns even where there is uncertainty. Early identification and reporting supports timely response and reduces potential harm.

1.6.12 Complaints

Concerns about privacy can be raised through MDQ's complaints process. MDQ responds to complaints in a timely and respectful manner. Where required, individuals may escalate concerns to relevant external authorities.

1.7 Communication

This policy will be:

- communicated to external stakeholders of MDQ, published on our website and client guide
- communicated to MDQ staff through induction and professional development opportunities;

1.8 Related Legislation & Documents

Related MDQ Policies/Documents

- Other policies included in this operations manual
- Policies contained in the Community Services Policies and Procedures Manual
- Feedback, Complaints, Incidents & Resolutions Policy
- MDQ Client Guide
- MDQ Website

National Legislation and Practice Standards

This policy is informed by, and applied in accordance with:

- **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**
- **Notifiable Data Breaches Scheme**
- **NDIS Act 2013 (Cth)**
- **NDIS Practice Standards and Quality Indicators**
- **Fundraising Institute of Australia (FIA) Code of Conduct**

- Relevant payment and financial data handling standards and obligations

State Legislation and Practice Standards

This policy is also informed by:

- **Information Privacy Act 2009 (Qld)**
- **Child Safe Organisations Act 2024 (Qld)** and the Queensland Child Safe Standards
- Other applicable Queensland legislation relating to service delivery, safeguarding and information management

1.9 Review of Policy

This policy will be reviewed:

- at least every two years, or earlier where required
- in response to changes in legislation, regulatory requirements or organisational practice
- following any significant privacy incident, data breach or identified risk

Reviews will ensure the policy remains current, effective and aligned with MDQ's Quality Framework and operational responsibilities across service delivery and fundraising activities.