



CLIENT INFORMATION AND GENERAL RECORDS POLICY

Applies to: Staff Members, Management Committee members and Volunteers/Students.

Specific responsibility: Manager and Management Committee.

Version: 1

Date approved: 17-Oct-2023

Next review date: Oct 2026

Policy context: This policy relates to

Legislation / Standards or other external requirements	- National Disability Insurance Scheme Act 2013 - National Disability Insurance Scheme (Provider Registration and Practices Standards) Rules 2018 - National Disability Insurance Scheme (Code of Conduct) Rules 2018 - National Disability Scheme (Protection and Disclosure of Information) Rules 2013 - National Disability Insurance Scheme (Approved Quality Auditors Scheme) Guidelines 2018 - Privacy and Personal Information Act 1998 - Children and Young Persons (Care and Protection) Act 1998, including Keeping them Safe – Chapter 16A - Health Records and Information Privacy Act 2002 - Commonwealth <i>Privacy Act 1988</i>. - Freedom of Information Act 1982
Contractual obligations	- Employment Agreements - Client Service Agreements and Schedule of Supports - NDIS Service Registered Service Provider obligations - DoE (Sector Capacity Building project contract) Funding Terms and Conditions (Funding Agreement).

POLICY STATEMENT

Early Connections- Manning and Great Lakes (EC-MGL) is committed to ensuring that it maintains and makes available client files and records in a manner which meets the requirements of relevant legislation and uses these records to promote effective service delivery to service users. EC-MGL is committed to transparency in its operations and to ensuring it is open to client and public scrutiny. It must also balance this with upholding the rights of individuals to privacy and of the organisation to maintain confidentiality regarding sensitive corporate matters.

Early Connections - MGL will prevent unauthorized persons gaining access to an individual's confidential records and permit individuals' access to their own records when this is reasonable and appropriate. Accordingly, access to some Early Connections - MGL documents and records will be limited to specified individuals and not be available to others for viewing.

This policy applies to the internal records, client records, personnel, organisational and unpublished materials of Early Connections - MGL. This Policy is guided by Legislation and aligns with the National Disability Insurance Scheme Act 2013, Privacy and Personal Information Protection Act 1998, NDIS Service Registered Service Provider obligations and the National Disability Insurance Scheme Standards, Rules, Policies, Guidelines, and the Code of Conduct.

PROCEDURES

1. Client and Staff information

1.1 Client files and records:

Files and records relating to each client will be maintained in a clear, objective, professional manner and will abide by confidentiality obligations. Client documentation will be recorded including:

- Intake documents – Service Agreement, Schedule of Supports, recording all client intake, client information and permission forms, risk assessments etc.
- NDIS claiming and Plan Manager correspondence,
- Service Reports for all client facing appointments,
- Service Plan reviews and meeting notes,
- Formal and informal reports,
- External stakeholder correspondence,
- Court Orders (if applicable)
- Phone call and email correspondence,
- Resource examples

All client records will be kept securely in electronic data storage (Echidna) and client files in staff only areas. These are updated, archived, and destroyed according to the organization's licensing requirements (NDIS Commission – Quality and Safeguards / Quality Audit – Audit participation process).

Client files and records are stored in the following locations:

1. Echidna Client Management program (Inetsolutions)
2. Staff Office 365 One Drive secure folder
3. Magnifi Finance and quoting system.
4. Minimal paper-based client file storage. Where used files stored in locked cabinet.

Security measures include:

- High level Australian security compliance and hosting. Daily encrypted backups across various locations ensure data is not lost. Further details are available on request.
- Two factor authentication for access and security level access depending on staff type.
- Staff access monitored and conflict of interest monitored. Where needed staff access restricted.
- IT company backup and monitoring

The destruction of paper files is managed through shredding bins at both centres. Files are shredded immediately or placed in a locked shredding bin for collection by a secure company. Destruction or archiving of electronic files- files archived or deleted from all areas e.g. documents, network, recycle bin and other drives after given timeframe.

1.2 Requests for access to Client Information and Records:

Clients / Parents / Legal Guardians have the right to:

- Access their records and advise the organisation about inaccuracies.
- Have your client record read only by the team directly involved in the delivery of your program OR in the Management team's monitoring of its quality.
- Expect all communication and other records pertaining to your service provision to be treated as confidential.
- Be provided with information on their right to access personal, private or confidential records containing information about their child and how they can request this.

Client records will be confidential to clients (or parent/legal guardian) and to all staff. Information about clients may only be made available to other parties with the consent of the child's parent/legal guardian, or in the case of legal subpoena.

Client record access will be granted where a written request for access is provided by authorized parent/guardian, no less than 14 days prior to access being given. This applies to all forms of client details including electronic files and hard copies (where retained).

Access to client records will be restricted for the following circumstances:

- where current Court Orders are in place,
- where information is stored for Mandatory Reporting (Child Protection) requirements,
- where there is significant concern of risk of harm,
- where parental disputes/ court order applications are pending or where reported domestic violence concerns are noted, some documentation may be restricted to protect private information of clients, such as personal contact information and appointment locations,
- staff notes such as clinical assessment scoring sheets that are used for data collection, however all resulting reports will be included, as per governing body requirements.

Requests for information about clients from outside agencies or individuals will be referred to Supervisor/Manager. Consent will be permitted only where client permission (primary caregiver) has been granted, unless permitted under Keep Them Safe - Chapter 16A.

Chapter 16A allows information to be exchanged between prescribed bodies despite other laws that prohibit or restrict the disclosure of personal information, such as the *Privacy and Personal Information Protection Act 1998*, the *Health Records and Information Privacy Act 2002* and the *Commonwealth Privacy Act 1988*. Chapter 16A allows for the exchange of information between prescribed bodies without Community Services involvement. In this Chapter, the term "organisation" applies to all "prescribed bodies", whether they are government or an NGO.

Client-related correspondence is required by EC-MGL with NDIA personnel and Agency partners, in accordance with NDIA requirements. This includes reporting, recommendations, equipment applications, claiming and audit requirements.

1.3 Recording and Storing of Video Files

From time to time team members may request that client families make video recordings of their child in their natural environment. Video files are a tool to help support Key workers, Teachers, Therapists and AHA's to observe, review and interpret children's skills and behaviour and family interactions. Video recordings can then be used to support the development of goals from client families Service Plans. Video recordings are particularly useful during times when families are accessing supports via Video Consults.

The following steps should be undertaken by all team members to ensure all video recordings are securely filed / stored:

- Client videos should only be sent to team members via email or via Microsoft TEAMS, which have the appropriate encryption to ensure client file security.
- Video recordings filmed by team members on phones, iPads or laptops need to be uploaded into the clients individual client folder after the client appointment and deleted from the device once uploaded.

1.4 Personnel/staff files

A personnel file is held in system storage (Employment Hero / KeyPay / One Drive secure storage) for each staff member and contains:

- contact details and emergency contact information in case of an emergency.
- a copy of the employee's contract and position description

- all correspondence relating to employment, pay and leave records, supervision, professional development certificates etc.
- Staff registrations, certificates, WWCC, NDIS Worker's Check, 100 pt ID, insurances etc.

Access to personnel information is restricted to:

- the individual staff member accessing their own file.
- the Manager
- the Finance Manager
- Direct Supervisor (applicable access only)
- Workplace management/Disciplinary action reports will be kept separately and can be requested by staff in writing no less than 14 days prior to access to files.

1.5 Appeals

Individuals who are refused access to their own records or information files may appeal by contacting the Manager who will review the decision in the context of this policy.

1.6 Freedom of Information Legislation

From time to time, Early Connections – Manning and Great Lakes may receive requests for information. These requests may include:

- clients or service users seeking to access information held about them.
- documents sought as part of a court proceeding - sometimes called 'discovery'.
- documents sought through a subpoena.
- information sought using Freedom of Information provisions (where services are linked to Government).
- members seeking access to the documents of your organisation, such as meeting minutes or financial records.

In these cases, we will follow the rules, regulations and record keeping requirements set out in the following - Freedom of Information Act

- Australian Charities and Not-for-profits Commission Act 2012 (ACNC Act), and
- Corporations Act 2001 (that charities must comply with before they are registered with the ACNC)

1.7 Access to Client Files for the NDIS Quality Audit

As an NDIS Service Provider it is a Legislative requirement that client files are accessed for the **NDIS Quality Audit** process. The external Auditor will request access to all client files. All client families will be advised of this process on enrolment and this information will be included in the Service Agreement. All Client families will be automatically included in the Audit process and will be notified in writing prior to an access request from the Auditor. At this time all client families will be given the option to "Opt –Out" of the Audit process. All **Audit-related documentation** will be filed in individual client files.

When conducting audits against the NDIS Practice Standards the approved quality auditor shall consider participants' experiences of supports as an important part of the triangulation of evidence. In the collection of evidence, the principles of sampling apply to the review of documents, interview attendee selection and observations. (National Disability Insurance Scheme (Approved Quality Auditors Scheme) Guidelines 2018).

<https://www.legislation.gov.au/Details/F2020C00100>

2. Organisational information

2.1 Management Committee

All papers and materials considered by the Management Committee will be open to Members of the Association following the meeting at which they are considered, except where the Management Committee deems it necessary to make any specific paper or material confidential.

Management Committee records are kept in same manner as client records in secure file storage locations by Manager, President, Treasurer and Finance Manager.

2.1 Early Connections - Manning and Great Lakes membership records

A list of current Early Connections - MGL Members of Association will be available on request to Early Connections - MGL members, Management Committee members. Personal information about members (including address and contact details) is confidential and may only be accessed by Manager and Management Committee.

2.3 Corporate records

Corporate records are those that contain confidential or commercially sensitive information about the organisation's business. They include:

- The financial accounts and records
- Taxation records
- Corporate correspondence
- Records of staff or other internal meetings
- Project management files
- Contracts between the organisation and other parties

Access to these records is limited to Manager, Management Committee and applicable personnel eg Accountant, Finance Manager, Assistant Manager, Funding Bodies etc.

2.4 Requests for access – general records

All records and materials not falling into the categories above may be released to the public at the discretion of the Manager and Management Committee.

Any request for access to information should be directed in writing to the Manager, who will:

- Make available to staff or Management Committee members information that they are entitled to access, or
- Refer any request from Early Connections - MGL members or the public for access to the organisation's records or materials to the Manager.

In considering a request, the Manager will take into consideration:

- A general presumption in favour of transparency.
- The relevant provisions of Early Connections - MGL constitution regarding information to be made available to Early Connections - MGL members.
- The business, legal, and administrative interests of Early Connections - MGL, including commercial confidentiality and privacy obligations.

Where an external party requests access to information that requires staff to devote time to collating, copying or otherwise making material accessible, the Manager may determine a fee to be charged.

2.5 Privacy Breach - Accidental or unauthorised disclosure of personal information

As a Registered Service provider for the NDIS, Early Connections – MGL must comply with the same quality privacy standards as the NDIS Commission – Quality and Safeguards. The Organisation will take seriously and deal promptly with any accidental or unauthorised disclosure of personal information of stakeholders, client families, members and employees. EC-MGL will use the same process for dealing with breaches of privacy as the NDIS Commission by following the OAIC's [Data breach notification — A guide to handling personal information security breaches](#) when handling accidental or unauthorised disclosures of personal information. Legislative or administrative sanctions, including criminal sanctions, may apply to unauthorised disclosures of personal information.

DOCUMENTATION

Documents related to this policy	
Related policies	- Confidentiality Policy - Child Protection Policy - Interactions with Children Policy - Financial Management System and Delegation Policy and Procedures - Risk Management Policy - Restrictive Practice and Behaviour Support Policy - Case Management Service Plan Policy - Access to Confidential Information Policy 2020 (Rescinded) - Client Records Policy 2020 (Rescinded)
Forms, record keeping or other organisational documents	- Your Information Its Private Brochure - Client Rights and Responsibilities Brochure - Intake Forms - Service Agreement & Schedule of Supports - Keeping Them Safe Documents - Client and Staff Files - Management Committee minutes - AGM minutes - Member of Association records.

Reviewing and approving this policy		
Frequency	Person responsible	Approval
Every 3 years or as needed	Manager and Management Committee	Management Committee

Policy reviews and version tracking			
Review	Date Approved	Approved by	Next Review Due
1	17 th Oct 2023	Management Committee	Oct 2026

The Management Committee
17-Oct-2023