Policy name	*Service Delivery Privacy and Confidentiality Policy*
Version	3.0
Responsibility	*Chief Executive Officer*
Date of development	*May 2017*
Date approved	*May 2017*
Date of next review	*Updated with each iteration of the policy; Annual review cycle, or following any reportable incident*
Relevant standards	*Privacy Act 1988* *National Disability Insurance Scheme Act 2013 (Cth)* *National Standards for Disability Services 2013 (Cth)*

Our Vision

To enhance lives and change perceptions of Down syndrome within society through dance, fitness and performance.

Purpose

This policy applies to all e.motion21 staff members, contract teachers and volunteers. e.motion21 will adhere to confidentiality, privacy and health records legislation.

Related Policy	**Forms**
Code of Conduct	*Confidentiality Agreement*
HR Framework	*Incident Report Form*
Workplace Bullying and Harassment Policy	
Anti-Discrimination and Equal Opportunity Policy	
Incident Reporting Procedure	
Mandatory Reporting Procedure	

Policy

e.motion21 understands that privacy and confidentiality is important to our community.

e.motion21 abides by and upholds the ten National Privacy Principles extracted from Schedule 3 of the *Privacy Act 1988* as amended to 14 September 2006. For detailed information pertaining to these principles refer to the Privacy Fact Sheet here - https://www.dropbox.com/s/ur7dheai845um80/privacy-fact-sheet-2-national-privacy-principles.pdf?dl=0 .

Unless otherwise required by law, confidential information will be treated as such, and personal information will be utilised only for the purpose intended. Such personal information will not be disclosed to any other organisations or to any other individuals without express permission from the individual to whom the details relate, except where the law requires such information to be divulged.

Principles

- All e.motion21 staff members' induction includes an orientation to privacy and confidentiality policy and practice and they are required to sign a confidentiality agreement.
- All personal or identifying information gathered and compiled in relation to service users will be kept in secure individual files (electronic or hard file) accessible to authorised staff members only.
- All service user files (electronic or hard file) remain the property of e.motion21. Inactive and closed files are retained and archived for a minimum of seven years by the organisation.

- All electronic data bases and computer based files will be accessible only on the e.motion21 computer system by authorised staff with current, individual password and user name.
- Service user consent must be obtained to retain information and to release information to nominated health professionals, carers, agencies or individuals.
- All service users will be provided on intake with information regarding their privacy and confidentiality (*Your Information – It's Private* *https://www.dropbox.com/s/f23vyrvjg44rgqi/e.motion21%20Service%20User%20Privacy%20Information.docx?dl=0*) including the storage and use of information, data required for reporting purposes and conditions where disclosure is permitted by legislation or duty of care.
- Information relating to a service user may only be disclosed without service user consent when required by law including:

  1. cases where mandatory reporting conditions exist;
  2. a valid search warrant is issued by law;
  3. when information is subpoenaed for court proceedings,
  4. where duty of care overrides confidentiality.
- Staff members should always consult a line manager and in the cases of subpoena, search warrant or court proceedings no information may be released without consultation with the Chief Executive Officer or their delegate.

Breaches

Breaches of confidentiality and privacy are considered serious disciplinary matters as they may result in harm to the service user, mistrust or discredit the organisation and will result in disciplinary, dismissal and / or legal action.

The Chief Executive Officer should be contacted if a breach occurs. If the Chief Executive Officer is suspected of involvement, or if the person who has formed the reasonable belief does not believe the matter is being appropriately addressed, the matter should be reported to the Chairman of the Board.

There are mandatory reporting requirements with regards to breaches of privacy. A 'Privacy Incident' may be a breach, a possible breach or a 'near miss'.

- **Breach or Possible Breach** – an action or omission that results in loss, theft, misuse or unauthorised disclosure of personal information, or has the potential to do so.
- **Near Miss** – are situations where a breach would have occurred without intervention. This includes situations where a privacy incident has occurred without any actual disclosure of personal information
- Where a complaint has been made that a privacy breach has occurred, which then needs to be investigated (all allegation of privacy breach).

Document history			
Date of review	***Reviewed/Revised by***	***Endorsed by***	***Notes***
May 2017	*Chief Executive Officer*	*Chief Executive Officer*	
June 2017, on advice from Quantum	*NDIS Project Officer*	*Chief Executive Officer*	

Certification Services			
January 2018	*NDIS Project Officer*	*Chief Executive Officer*	*Board reviewed and accepted changes made due to legislative requirements*