

Policy name & ID code	<i>Privacy and Confidentiality Policy - QM 5.0</i>
Version	Draft V4
e.motion21 and Impact21	<i>All references to e.motion21 is inclusive of all e.motion21 programs including but not limited to Impact21 unless otherwise specifically stated</i>
Responsibility	<i>Chief Executive Officer</i>
Date of currency	<i>August 2020</i>
Date of next review	<i>April 2022 or following a change in related regulation or guidelines or a reportable incident</i>
Relevant standards	<i>NDIS Quality and Safeguards Commission – July 2019 NDIS Practice Standards and Quality Indicators – Jan 2020 Version 3 Office of the Australian Information Commissioner reportable data breach requirements</i>
Relevant act.	<i>National Privacy Principles extracted from Schedule 3 of the Privacy Act 1988 as amended to 14 September 2006</i>

Our Vision

We believe in an inclusive future where people with Down syndrome and intellectual disability are flourishing and active contributors to society economically, socially and creatively. We do this through Moving Bodies, Moving Boundaries and Moving Minds. This is what we stand for, and how we are making Australia a better place.

Through dance, fitness, education and employment programs we are enhancing lives and changing perceptions of Down syndrome and intellectual disability within society.

Purpose

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

Related Policy	Forms
<i>Code of Conduct</i>	<i>Confidentiality Agreement</i>
<i>Human Resources Procedure</i>	<i>Incident Report Form</i>
<i>Workplace Bullying and Harassment Policy</i>	
<i>Diversity and Equal Opportunity Policy</i>	
<i>Abuse and Neglect Policy</i>	
<i>Incident Reporting Procedure</i>	
<i>Complaints and Feedback Policy & Procedure</i>	

Policy

e.motion21 understands that privacy and confidentiality are 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.privacy.org.au/Resources/NPPs-140311.pdf>

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 individual without written prior permission from the individual to whom the details relate, except where the law requires such information to be divulged.

Principles

- All e.motion21 staff, contractors and volunteer 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 participants will be kept in secure individual files (electronic or hard copy) accessible to authorised staff members only
- All participants' files (electronic or hard copy) 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 electronic

information management system by authorised staff with a current, individual password and user name

- Consent from the participant or their key support person must be obtained to retain information and to release information to ~~other~~ health professionals, carers, agencies or individuals
- Consent from the participant or their key support person must be obtained on enrolment for all visual and auditory recording of any aspect of e.motion21 events or my participation (this includes mobile phone photos/videos)
- All participants will be provided on enrolment with information regarding their privacy and confidentiality, 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 participant may only be disclosed without service user consent when required by law including:
 - cases where mandatory reporting conditions exist
 - a valid search warrant is issued by law
 - when information is subpoenaed for court proceedings
 - where duty of care overrides confidentiality, if a participant is at risk to themselves or others
- 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 participant, cause distrust of and/or discredit the organisation and will therefore result in disciplinary action, dismissal and/or legal action. This could be considered a reportable incident.

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 Chair 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.
- **Data Breach** – personal information is accessed or disclosed without authorisation or is lost
- **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 allegations of a privacy breach).

Reportable Breaches

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious harm to one or more individuals
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action
- An organisation or agency that suspects an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual.

If a data breach occurs it must be reported to the affected individuals and the Office of the Australian Information Commission. <https://www.oaic.gov.au/privacy/notifiable-data-breaches/>

If the breach may or did cause harm to the participant this would also be a reportable incident to the NDIS Commission. Following the Reportable Incident procedures.