Policy name & ID code	*Privacy and Confidentiality Policy - QM 5.0*
Version	Draft V5
Responsibility	*Chief Executive Officer*
Date of currency	*May 2022*
Date of next review	*April 2024 or following a change in related regulation or guidelines or a reportable incident*
Relevant standards	*NDIS Quality and Safeguards Commission – July 2019* *NDIS Practice Standards and Quality Indicators – Nov 2021* *Office of the Australian Information Commissioner reportable data breach requirements*
Relevant act.	*National Privacy Principles extracted from Schedule 3 of the Privacy Act 1988 as amended to 14 September 2006*

Our Vision

The Inclusion Foundation is a for-purpose-charity that champions the inclusion of people with Down syndrome. We see an inclusive world where people with Down syndrome are equal, active and respected members of society. Together, we stand proud, we raise our hands in the air, and we say to society, to business, to governments, to everyone, and to anyone… Count me in!

Purpose

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

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

Policy

Inclusion Foundation understands that privacy and confidentiality are important to our community.

Inclusion Foundation 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 Inclusion Foundation 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 Inclusion Foundation. 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 Inclusion Foundation electronic information management system by authorised staff with a current, individual password and username
- Consent from the participant or their key support person must be obtained to retain information and to release information to nominated 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 Inclusion Foundation 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.

Document history				
Location of Master - 2022 Priv&Confid Policy.docx				
Review date	***Version***	***Reviewed by***	***Endorsed by***	***Notes***
May 2017	*V1*	*CEO*	*CEO*	
June2017	*V2*	*NDIS PO*	*CEO*	*on advice from Quantum*
June 2020	*V3.*	*Program Director*	*CEO & FARM Chair*	*Made inclusive of Impact21* *Updated the vision statement* *Made current with the NDIS Quality and Safeguards Commission registration requirements and NDIS Practice Standards 2020 V3* *Added in data breach reporting requirements*
May 2022	*V4*	*SS Manager*	*CEO*	*Updated branding and organisation name to Inclusion Foundation* *Updated the vision statement* *Updated dates to most current legislature*
Approved for Publishing by CEO			*Date:*	*Signature:*