INFORMATION MANAGEMENT POLICY

1. PURPOSE

The purpose of this policy is to ensure Lift Up Voices operates effective communication processes and information management systems in accordance with legislative, regulatory compliance and organisational standards.

The policy has been framed around the individuals' rights as they are specified in the Privacy Act (1988), Freedom of Information Act (1982), Disability Services Act (1993) and NDIS Practice Standards *Provider Governance and Operational Management* Core Module 2 (Information Management). It also aligns with the Notifiable Data Breaches (NDB) Scheme, and the NDIS Amendment (Getting the NDIS Back on Track No.1) Act 2024.

2. SCOPE

It is the policy of Lift Up Voices that all participants, staff, contractors and volunteers will have records established upon entry to the service and maintained whilst active at Lift Up Voices. This includes external contractors, casual workers and students engaged in participant-related tasks.

3. POLICY

- Lift Up Voices will maintain effective information management systems that keep appropriate controls of privacy and confidentiality for stakeholders
- Lift Up Voices Policies and Procedures are kept as read-only documents in the Policies and Procedures folder on the shared drive and are available to access/view on the Lift Up Voices website
- Lift Up Voices' Directors are responsible for maintaining the currency of this information
- A copy of each form used by our organisation is maintained in the shared drive in the sub-folder; entitled "Forms & Docs".
- All staff can access the Policies and Procedures at Lift Up Voices in electronic format via the shared drive or on the Lift Up Voices website
- Policies and procedures are reviewed on a regular basis and maintenance of reviews is listed on the Policies and Procedures Register

4. PROCEDURES

4.1 Information Management System

4.1.1 Participant Documentation Procedures

- Confidentiality of participant's records is maintained
- Participant's files will provide accurate information regarding their services and support and will contain, but is not limited to:
    - Participant's personal details
    - Referral information
    - Assessments and progress notes
    - Support plans and goals
    - Participant's reviews
    - Details regarding service responses

- Original participant documentation will be stored on Splose and Lift Up Voices shared drive
- Information relating to participant's ongoing situation, including changes to their situation is to be documented in the participant's progress notes on Splose
- All Lift Up Voices workers required to document the activities relating to support of participants will be appropriately trained in documentation and record-keeping
- Individuals are not permitted to document on behalf of another person
- Participant's records will be audited regularly to ensure documentation is thorough, appropriate and of high quality
- Participant records will be stored in a safe and secure location with access available to authorised persons only
- Workers must ensure that all relevant information about the progress of or support provided to a Participant is entered into that person's file notes in a factual, accurate, complete and timely manner
- Workers must only use information collected from a participant for the purpose for which it was collected
- Participants, family and advocates have a right to access any of their personal information that has been collected. Workers will support such persons to access their personal information as requested.

4.1.2 Entering Lift Up Voices' Service

- All Participant personal and service information is to be collated during their initial consultation. This will only contain material relevant to the management of services or support needs, including but not limited to:

    - NDIS Service Agreement and Support Plan (developed in conjunction with the participant, their advocate(s) and any other family or service providers/individuals)
    - Session Reminders

- Consult Template
- Artist Profile
- Client Consent Form
- Media Consent
- Heath Care Plan (if required)

- Collect only personal information necessary to assess and manage the participant's support needs

4.1.3 Ongoing Documentation Procedures

- Maintain participant information in Splose (online staff portal) in accordance with system practices
- Document participant's information, service activities and progress only on Lift Up Voices approved forms or tools
- Clearly document:
    - The outcomes of all ongoing participant's assessments and reassessments
    - Changes or redevelopment of Participant's Support Plans, including revised goals or preferences
    - Any critical incidents or significant changes in the participant's health or well-being
    - Conversations (in person or via telephone) with the participant, family members, their representative or advocate
    - Conversations regarding the participant, with any other providers, agencies, health/ medical professionals, family members or other individuals with interest in the participant
    - Activities associated with the participant's admission and exit, including referrals

- Directors must regularly audit the files of participants to ensure that:
    - The file is up to date
    - All forms are being used appropriately
    - Non-current information is being culled and updated
    - The progress/file notes are factual, accurate, complete and in chronological order

4.1.4 Security of Files and Participant Information

- All current hard copy files for participants must be kept in a secure area, such as a lockable cabinet to ensure that only authorised personnel can gain access to personal information of a participant
- Authorised personnel include Lift Up Voices' workers who are employed or engaged to provide support to the participants
- All electronic files must be password protected to ensure confidentiality and security
- Where sensitive health or behavioural information is stored, access permissions must be limited to need-to-know personnel only.

4.1.5 Access to Participant's Files

Participants and/or their guardians must have access to their own records on request - the staff member responsible for delivering the service should approve and control the way participants access their files to ensure that the security of other non-related information is maintained.

Access to the participant's files is the direct responsibility of the staff member responsible for delivering the service. When access is requested by anyone other than workers employed or engaged by Lift Up Voices it will only be granted when a Director is satisfied with that the policies and procedures of Lift Up Voices has been followed, and access to the file is in the best interest of the participant. Such access will only be granted when the appropriate person has given consent.

All the participant's administration files are the property of Lift Up Voices and, although participants and their guardians can access the file, it cannot be taken by the participants or their guardian or be transferred to any service external to Lift Up Voices without permission of a Director. The proper procedure for releasing information about participants to persons or services that are external to Lift Up Voices is to proceed as per the *Privacy and Confidentiality Policy* and participant *Client Consent (built into Service Agreements).*

4.2 Staff Records

Staff files are kept on Splose (online portal), One Drive and Lift Up Voices' administration drive and are available only to the Directors. Each staff member has access to their individual staff file via One Drive.

4.3 Minutes of Meetings

Minutes of meetings are maintained electronically and are sent via email to those concerned and available upon request. Where meetings include discussion of participant-related matters, minutes must be stored securely and treated as confidential records.

4.4 Other Administrative Information

- Individual staff members are responsible for organising and maintaining the filing of general information in accordance with their job descriptions
- Administrative information including funding information, financial information and general filing are maintained electronically

4.5 Electronic Information Management

4.5.1 Data Storage

Data is stored in the following platforms:

Platform	File / Type of Information
One Drive	• Participant Progress Reports • Staff files • Administrative files • Communication to/from participants and their support network • Policies and Procedures • Registers • Staff PD files/documents
Splose	• Participant and staff contact information • Participant progress/session notes • NDIS Service Agreement and Support Plan • Client Consent Form (built into SA) • Media Consent (build into SA) • Session Reminders (built into SA) • Artist Profile • Heath Care Plan (if required) • Communication to/from participants and their support network
Cognito Forms	• Artist Profile • Consult Template • Staff Code of Conduct Acknowledgement Forms • Participant Feedback Forms
Google Drive	• Individual Mentoring Program Plans • Staff Mentoring Program Handbook
Xero	• Financial information (quotes, invoices)

All platforms must be reviewed regularly to ensure they continue to meet data protection and compliance standards.

4.5.2 Data Backup

All computer data is automatically backed up to One Drive. Lift Up Voices will regularly verify backup functionality and ensure secure offsite/cloud storage is functioning correctly.

4.5.3 Email

- All staff are to use their Lift Up Voices email for work related communication only
- Pornographic, sex-related or other junk email received is to be deleted immediately
- Emails containing sensitive or personal information must be encrypted where possible and never forwarded outside Lift Up Voices unless authorised.

4.5.4 Internet

- Internet access is restricted to work-related purposes
- Under no circumstances are workers allowed to access pornographic or sex-related sites

4.5.5 Getting Help and Reporting Problems

If staff experience problems with a program or computer or any other piece of equipment, they can contact a Director for assistance. All IT or data breaches (e.g. lost/stolen devices, unauthorised access, malware) must be reported to a Director immediately.

4.5.6 Social Media

We are aware that social media (social networking sites; Facebook, Twitter or similar, video and photo-sharing sites, blogs, forums, discussion boards and websites) promotes communication and information sharing.

Staff who work in our organisation are required to ensure the privacy and confidentiality of the organisation's information and the privacy and confidentiality of the participant's information. Staff must not access inappropriate information or share any information related to their work through social media sites. Staff are required to seek clarification from a Director if in doubt as to the appropriateness of sharing any information related to their work on social media sites.

Organisational social media posts involving participants must have written consent via a Media Consent form (built into Service Agreements).

4.6 Monitoring Information Management Processes and Systems

Information management processes and systems are regularly audited as part of our audit program. Staff, participants and other stakeholders are encouraged to provide ongoing feedback on issues and areas where improvements can be made.

Regular audits are conducted in line with the Quality and Safeguards Commission's expectations and will inform continuous improvement. Where risks are identified (e.g. data breach risks or file inaccessibility), Directors will action corrective steps and document these in the Continuous Improvement Register.

5. REVIEW

This policy will be reviewed every two years. If at any time the legislative, policy or funding environment is so altered that the policy is no longer appropriate in its current form, the policy will be reviewed immediately and amended accordingly. This includes changes to the Australian Privacy Principles, NDIS reporting requirements or cyber security legislation.

RELATED POLICIES

Code of Conduct Policy
Privacy and Confidentiality Policy
Service Delivery Policy
Abuse, Neglect and Exploitation Policy

RELEVANT LEGISLATION OR STANDARDS

National Disability Insurance Scheme Act (2013)
NDIS Practice Standards and Quality Indicators (2020)
NDIS Amendment (Getting the NDIS Back on Track No.1) Act 2024
Privacy Act 1988 (Australian Privacy Principles)
Notifiable Data Breaches (NDB) Scheme
Freedom of Information Act 1982