PLAY GROW FLOURISH PTY LTD
NDIS Support services

Privacy and Confidentiality Policy and Procedures

"I have the right to understand what information is being collected and what it will be used for" – client voice

Introduction

Play Grow Flourish is committed to safeguarding the confidentiality of personal or sensitive information collected about the people they support. Play Grow Flourish respect and protect client's and staff member's dignity and right to privacy.

Each person is advised of the confidentiality policies using the language, mode of communication, and terms they are most likely to understand.

Play Grow Flourish has developed specific procedures to effectively manage personal information, including sensitive information, in the context of the services provided.

Scope

All management, staff, contractors, students, and volunteers of Play Grow Flourish have a responsibility to ensure that personal information is handled according to this policy and that they are bound by their commitment to confidentiality. All contractors, students and volunteers must also complete induction training related to privacy and confidentiality before engaging in service delivery. They are held to the same standards as permanent staff and must sign a confidentiality agreement before beginning their role.

Principles

Play Grow Flourish is respectful of clients' information and clients' right to privacy. Play Grow Flourish strives to achieve the safest and most highly protected methods of securing information to protect the privacy of clients and staff (see also *Information Management Policy and procedure).*

Legislative context

Play Grow Flourish abides by its record-keeping obligations. Legislation that relates to privacy is:

- Privacy Act 1988
- Public Records Act 1988
- National Security Legislation Amendment Act (no.1) 2014
- Privacy Amendment (Private Sector) Act 2000
- National Privacy Principles (2001)
- Privacy and Personal Information Protection Act 1998 (NSW)

- NDIS (Protection and Disclosure of Information) Rules 2013

Policy

This policy sets out how Play Grow Flourish complies with obligations under the Privacy Act 1988, including the Australian Privacy Principles, to ensure legal and ethical obligations are met to respect the rights and privacy of clients and staff.

This policy regulates how Play Grow Flourish collects, uses, and discloses personal information. It also details how individuals may access that information as required.

Collecting and holding personal information

Play Grow Flourish will take all reasonable steps to ensure that the personal and/or sensitive information it collects, uses, or discloses is accurate, complete, and up to date. Personal or sensitive information about clients will only be collected when it is directly relevant and needed to provide support services to that person or where Play Grow Flourish is required to collect that information.

Procedure

Play Grow Flourish has procedures to allow clients and staff to access information stored about them, update and or amend their information on file.

Digital Security and Devices

All staff must ensure that electronic devices used to access client or staff information are secured with passwords or biometric locks. Use of personal phones or email accounts for work purposes is discouraged unless approved by management. Digital files containing personal information must be stored in secure cloud systems approved by the organisation (e.g. Brevity, Deputy, Xero). Any loss or unauthorised access of device must be reported immediately. Staff must not share, post, or comment on any content related to clients, other staff members, or internal organisational matters on social media or public forums, even in closed or private groups. This includes indirect references or posts that could identify individuals or sensitive incidents.

Information generally collected about a person includes:

Personal information collected and held may include, but is not limited to name, date of birth, gender, address, residency status, contact number, email address, emergency contact details, NDIS plan, audio/visual information, and cultural background. Information may also include specific behaviour support needs or medication requirements. Play Grow Flourish also hold support notes that outline each client activities and observations during support.

Health information collected may include:

- Medical information, when this is collected or used in connection with delivering services to clients, or to understand any impacts it may have on the individual.

- Information generated by a health service provider, such as management plans, medication and any professional advice about a client and their health.

Play Grow Flourish may collect personal information:

- Directly from the client – verbally or in writing and is recorded.
- From third parties, such as medical practitioners, government agencies, a client's representatives, carer, and other health service providers
- From client referrals

Play Grow Flourish will:

- Explain what information will be collected and why including recorded material in audio/and or visual format.
- Obtain consent from the client during the intake process to collect information as required.
- Collect information necessary to support a role, functions, or activities within Play Grow Flourish services.
- Collect sensitive information directly from the person if it is reasonable and practicable to do so.
- Use fair and lawful ways to collect sensitive information, and not in an intrusive manner.

Who collects this information?

Play Grow Flourish staff collect personal and sensitive information their normal duties and for the organisation's use. Play Grow Flourish generally collects personal and sensitive information directly from the relevant person through standard forms, over the internet, via email, face-to-face meetings, or telephone conversation. With the person's consent, Play Grow Flourish may collect personal and sensitive information from third-party contractors or agents and government instrumentalities involved in providing services.

Collection of personal information – Play Grow Flourish staff

All information supplied by staff will be placed on their personnel file, which may be held in both electronic and hard copy format. Both formats are securely held, with access only available to the Director or third-party assessors for audit purposes.

Why is personal information collected?

Client's personal information is used to:

- Assess and provide the services that are required.
- Administer and manage those services.
- Evaluate and improve the services offered.
- Contact family, carers, or other third parties as and if required.

- Meet obligations required for compliance.
- Analyse services and client needs with a view to developing new or improved services.

Staff or potential staff member's information is used to:

- Assess employment applications.
- Obtain and Monitor screening requirements.
- Process payment of salaries and meet legislative obligations such as the payment of superannuation and taxation.
- Provide duty of care in employment
- Contact family, carers, or other third parties as and if required.
- Ensure personnel hold a current driver's licence and private motor vehicle registration as required to perform roles.

If Play Grow Flourish is not able to obtain personal information, it may limit their ability to provide a quality service or meet duty of care and legislative responsibilities as an employer and service provider.

Disclosing personal information

Play Grow Flourish will uphold a clients' right to privacy and confidentiality to the extent that it does not impose a serious risk to the client or others. As above, Play Grow Flourish may disclose clients' personal information to other people or organisations with the client's consent.

This may include disclosure to:

- Medical and allied health service providers
- A 'person responsible' if the client is unable to give or communicate consent. In some instances, verbal consent from a Person Responsible may be necessary and will be documented.
- The client's authorised representative/s e.g. legal adviser
- Play Grow Flourish professional advisers (e.g. lawyers, accountants, auditors).

Consent is not required for release of information to:

- Government and regulatory authorities where harm is present.
- When required or authorised by law or related to a criminal issue.

Where there is uncertainty as to the direct benefit of the release of information which does not remove the names of individuals and or other identifying characteristics such as a home address, or there is doubt that individuals would not consent to the release of information Play Grow Flourish will seek approval from the concerned people or the designated person responsible before the release of the information.

Accessing personal information

Staff and clients can request and be granted access to their personal information, subject to exceptions allowed by law. Any requests for access to personal information must state what information is to be accessed and how they wish to access the information. A request to access personal information from clients should be forwarded to the Director in writing. If a staff member wants to request access to their file, they can do so by putting their request in writing to their Director.

Should the Director decide that access to personal information will not be provided, they must put the reasons for the refusal and the mechanisms available to complain in writing to the staff member or client within 30 days of receipt of the request. Should access be granted, the Director must contact either the staff member or client and arrange for access to their personal information, based on the method of access requested within 30 days of receipt of the request.

Should Play Grow Flourish not be able to provide the data in the method requested, the Director is to discuss with the staff member or client, alternative methods available to access their personal information.

Photographs and videos

Photographs and videos are classified as personal information under privacy legislation.

Play Grow Flourish will ensure all clients, or their nominated family member sign a media consent (or non-consent) form prior to receiving services.

Consent will also be sought from clients where any media is likely to be shared through text, ensuring that the client understands and agrees to what will be shared in what kind of format, and the reasons why it is being shared.

Breach of privacy

Where Play Grow Flourish become aware of a breach of privacy, the Director will immediately assess the incident to determine if it is likely to result in serious harm to the individual. Where it is likely, Play Grow Flourish will immediately notify the Office of the Australian Information Commissioner Notifiable data breaches — OAIC where:

- 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, and
- Play Grow Flourish has not been able to prevent the likely risk of serious harm with remedial action

Privacy Breach Response

Any suspected or actual breach of privacy must be reported immediately to the Shift Manager or Management team.
Management will assess the nature and severity of the breach, take remedial action, and determine whether the breach must be reported to the Office of the Australian Information

Commissioner (OAIC) under the involved will be supported through the review process and any necessary corrective measures.

Training

All staff are trained in Privacy and Confidentiality procedures during their induction. On completion of training, a Code of Conduct is signed as a commitment to maintain confidentiality when undertaking a role for Play Grow Flourish.

Ongoing Awareness

All staff are expected to remain up to date with privacy and confidentiality expectations. Management may schedule annual refresher training, team discussions, or staff briefings to reinforce procedures. Shift Managers are responsible for monitoring daily practices and supporting staff to stay compliant.

Responsibilities

For the purpose of this policy the Management team or Management includes the Director, Executive Team Leader and the Human Resources Manager.

Management is responsible for:

- Maintaining this policy its related procedures and associated documents.
- Ensuring the policy is effectively implemented across the service.
- Providing access to client where the person has requested it.
- Reporting to the OAIC where a notifiable breach has occurred
- Reviewing staff access permissions to ensure only authorised individuals access sensitive information.
- Ensuring privacy and confidentiality training is included in ongoing professional development plans.
- Maintaining oversight of how third-party systems (e.g. Deputy, Brevity and Xero) are used to store and access personal information.
- Supporting internal audits and risk assessments to specific to data handling and storage.
- Monitor staff compliance with the requirements of the policy.

Shift Managers are responsible for:

- Ensure training and information is provided to staff to ensure clients are advised of their right to privacy and information is managed in line with the *Information Management Policy*
- Providing access to team information where the person has requested it.

- Ensuring that all clients are explained their right to privacy and sign a consent form.
- Not discussing client information outside of their role requirements
- Ensuring ongoing security of client information when accessing, storing, retrieving, or disposing of client information.
- Supporting staff to complete privacy-related documentation (e.g. consent forms, access requests)
- Ensuring team access to privacy tools, such as locked filing cabinets or secure digital folders.
- Regularly reviewing staff knowledge of privacy procedures and identifying where refresher training is needed.
- Ensuring only relevant staff are present during discussions or debriefs involving sensitive client matters.
- Liaising with Management when unsure if client information should be disclosed or withheld.

Staff are responsible for:

- Ensuring ongoing security of client information when accessing, storing, retrieving, or disposing of client information.
- Reminding clients of their right to privacy
- Not discussing client information outside of their role requirements
- Documenting and notifying the Shift Manager of any suspected instances where a breach of confidentiality has occurred.
- Taking all reasonable steps to ensure that client files, forms, notes and media are not left unattended or visible to unauthorised persons.
- Avoiding the use of personal phones or devices to capture, store or share any client related information, unless explicitly approved and compliant with service protocols.
- Ensuring that client-related discussions (including behaviours, support needs or family information) are only held in private and professional settings, never in public areas or with other clients present.
- Immediately reporting any accidental or intentional sharing of personal information (verbally, digitally, or in writing) to their Shift Manager or Managements before sharing any information externally, even with family members or external providers.
- Following correct procedures when disposing of printed documents containing personal information (e.g. shredding or placing in secure disposal bins).
- Seeking clarification from a Shift Manager or Management before sharing any information externally, even with family members or external providers.

- Maintaining strict confidentiality when supporting clients shared environments, including being mindful of conversations, client records or visible support materials in group settings.
- Refraining from sharing client's anecdote photos, situations with others (even casual) that could lead to identifications or breach of trust.
- Refraining from discussing internal matters, operational decisions, client information or staff-related concerns with former employees or individuals who are no longer affiliated with the organisation. This includes both casual conversations and intentional disclosures, regardless of setting or perceived risk.
- Understanding that confidentiality extends beyond the period of employment and applies to all information obtained in the course of their role, including after staff have left the organisation.

Related Policies and Documents

- Information Management Policy and Procedure
- Risk Management Policy and Procedure
- Consent Form
- Complaints and Feedback Policy and Procedure
- Human Resources Policy and Procedure
- Code of Conduct

Review

Play Grow Flourish will review each policy through internal audit processes, client feedback or as contextual drivers determine the need for a review.

Release Date:	Version No:	Approved By:	Amendments:
January 2024	1.0	Director	Nil
Review Date:	**Version No:**	**Approved By:**	**Amendments:**
May 2025	2.0	Human Resources Manager	Additional responsibilities added for Management, Shift Managers, and Staff in response to a recent privacy breach. New clauses introduced on digital device security, social media use, conversations with former staff and privacy breach response. Full details recorded in the Master Register.