EASTWOOD HEIGHTS OOSH

Confidentiality and Privacy Policy

Policy Number	QA7/4	**Title**	Confidentiality and Privacy Policy
Revision	2.0	**Written By**	Policy Team and Nominated Supervisor
Reviewed By	EHOOSH Management Committee	**Approved By**	EHOOSH Management Committee
Supersedes	1.2	**Effective Date**	February 2025

1. Policy Statement

Eastwood Heights OOSH is committed to protecting the privacy and confidentiality of all individuals associated with the service, including children, families, educators, and staff. The service recognises the importance of maintaining secure, respectful, and professional relationships where families can trust that their personal information is managed appropriately. The collection, storage, use, and disclosure of personal and sensitive information are conducted in compliance with the Privacy Act 1988, the Education and Care Services National Law Act 2010, and the Education and Care Services National Regulations 2011 to ensure that all information is handled with integrity and in accordance with legal requirements.

This policy upholds the principles outlined in National Quality Standard (NQS), which mandates that educational and care services implement governance procedures that are effective and compliant with legislative requirements. It establishes guidelines for the responsible management of personal information, ensuring that privacy is respected, data is

securely stored, and access is granted only to authorised personnel who require it to fulfil their duties.

2. Background

The Education and Care Services National Regulations require policies and procedures to be in place in relation to confidentiality and privacy.

3. Procedure

The following procedures outline the practical steps and responsibilities for ensuring the confidentiality and privacy of personal information within the Service. These procedures define the obligations of staff and management in handling personal data, preventing unauthorised disclosure, and ensuring compliance with legal requirements. The implementation of these procedures promotes a secure and professional environment where sensitive information is managed responsibly.

3.1. Collection Of Personal Information

The Service will collect personal information in a lawful, fair, and unobtrusive manner, ensuring that all information gathered is directly relevant to the operation of the Service and the safety, wellbeing, and development of children in care. Families, staff, and relevant authorities will be informed at the time of collection about the purpose for which their information is required, how it will be stored and used, and their rights to access and update personal details. Personal information collected includes, but is not limited to, enrolment details, emergency contact information, medical histories, immunisation records, and staff employment details.

The collection of personal information will be limited to what is necessary for the effective administration of the Service. Information will not be collected unlawfully or without the knowledge of the individual concerned, except where required by law.

3.2. Storage and Security of Information

All personal and sensitive information will be stored securely to prevent unauthorised access, loss, misuse, or disclosure. Physical records will be kept in locked filing cabinets, while digital

records will be stored on Hub Hello. Access to confidential records will be restricted to authorised personnel, including the Approved Provider, Nominated Supervisor, and other designated individuals who require access to fulfil their roles (RPIC's).

The Service will ensure that children's records are retained for a minimum of three years after the last date of attendance, while staff employment records will be maintained for a minimum of seven years after the individual ceases employment. When records are no longer required, they will be securely destroyed by shredding physical documents or permanently deleting digital files in compliance with privacy legislation.

3.3. Use and Disclosure of Information

Personal information collected by the Service will only be used for the primary purpose for which it was obtained. Information will not be disclosed to third parties without the written consent of the individual or their authorised representative, except where required or authorised by law. Information may be disclosed to regulatory bodies, child protection authorities, or emergency services when necessary to prevent serious harm to a child, staff member, or the public.

The Service strictly prohibits the unauthorised sharing of personal information, including the use of photographs or identifying details on social media platforms or in public forums, without explicit written consent from families. Any visual images of children, including photographs and videos, will only be taken, stored, or used for educational and operational purposes with prior parental approval.

3.4. Access to Personal Information

Individuals have the right to access their personal records upon request. Requests must be submitted in writing to the Approved Provider or Nominated Supervisor, who will arrange a time for the individual to review their records in a secure and supervised setting. Before access is granted, the Service will verify the identity of the applicant to ensure that no confidential information about other individuals is inadvertently disclosed.

3.5. Retention and Disposal of Records

The Service will retain all required records for the legally mandated periods. Children's

records, including enrolment and medical information, will be kept for at least three years following their last day of attendance. Personnel records, including employment contracts and payroll details, will be retained for seven years after an individual's employment ceases. Once these periods have expired, all records will be securely destroyed to protect individuals' privacy.

3.6. Handling Complaints and Privacy Breaches

Any concerns or complaints regarding privacy and confidentiality should be directed in writing to the Approved Provider or Nominated Supervisor. The Service will investigate all complaints promptly and implement necessary corrective actions. If an individual remains dissatisfied with the outcome, they may escalate the matter to the Office of the Australian Information Commissioner (OAIC).

In the event of a significant privacy breach, the Service will adhere to the Notifiable Data Breaches (NDB) scheme, which requires that affected individuals and regulatory authorities be informed if there is a serious risk of harm resulting from the breach.

4. Roles and Responsibilities

Approved Provider	• Ensure compliance with all relevant privacy legislation and regulatory requirements. • Review and approve the Confidentiality and Privacy Policy. • Oversee the lawful and ethical collection, use, and storage of personal information. • Ensure appropriate procedures are in place for handling privacy breaches and complaints.
Nominated Supervisor	• Implement the Confidentiality and Privacy Policy within the Service. • Ensure all educators and staff understand and comply with confidentiality requirements. • Manage requests for access to personal information • Maintain accurate records of access requests and ensure they are processed securely.

	• Investigate and manage any breaches of privacy, ensuring corrective action is taken. • Restrict access to confidential information to authorised personnel only. • Oversee the secure disposal of expired records • Store personal records securely and prevent unauthorised access.
Responsible Person in Charge	• Support the Nominated Supervisor in implementing this policy. • Ensure that personal information is handled securely and in accordance with this policy during their period of responsibility. • Collect, use, and disclose personal information only as necessary and in accordance with this policy.
Educators and Support Staff	• Maintain the confidentiality of personal information in all professional interactions. • Report any suspected privacy breaches to the Nominated Supervisor immediately. • Adhere to policies restricting the unauthorised sharing of information, including on social media platforms.
Families	• Provide accurate and up-to-date personal information as required for enrolment and the provision of services. • Inform the Service of any changes to personal information in a timely manner. • Respect the privacy and confidentiality of other families, children, and staff within the Service. • Raise any concerns or complaints about privacy issues through the appropriate channels.

5. References

5.1. Statutory Authority

- Privacy Act 1988
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011 (Regulation 181, 183)

5.2. Relevant Service Policies

- Child Protection Policy
- Grievances and Complaints Policy
- Governance and Management Policy
- Service Access Policy

5.3. National Frameworks

- National Quality Framework (NQF)
- Early Years Learning Framework (EYLF)
- My Time, Our Place (MTOP)
- Child Safe Standards (NSW)

6. Legislative Requirements.

Education and Care Services National Law Act 2010 & Education and Care Services National Regulations 2011

Section 175	Offence relating to protection of children from harm and hazards
Section 269	Protection of personal information
Regulation 181	Confidentiality of records
Regulation 182	Written consent required for disclosure of information
Regulation 183	Storage of records and documents
Regulation 168	Policies and procedures required

Revision Chronology

Version Number	Date	Reason for Change
1.0	October 2018	Endorsed by OOSH executive committee
1.1	March 2021	Review and evaluation
1.2	April 2021	Edited and reviewed
2.0	February 2025	Edited, reviewed with new policy template