Privacy, Confidentiality & Information Management Policy & Procedure

Applies to: All employees, contractors, volunteers, Board members and clients of Koorana Child & Family Services Limited.	**Version: 5**
Purpose: Provide guidance and establish processes to protect the privacy, dignity and confidentiality of the persons associated with Koorana.	**Date approved: 01/12/2025**
	Next review date: 01/12/2026
	Approved by: CEO

Policy context: This policy relates to	
Standards or other external requirements	▪ Australian Privacy Principles ▪ Privacy and Other Legislation Amendment Act 2024 ▪ National Disability Practice Standards and Quality Indicators ▪ Fair Work Act ▪ Fair Work – Workplace privacy best practice guide (Fair Work Ombudsman) ▪ National Principles for Child Safe Organisations (Australian Human Rights Commission)
Legislation or other requirements	▪ NDIS Framework ▪ NQS Framework ▪ NDIS Code of Conduct ▪ Privacy Act 1988 (Cth) ▪ Privacy and Personal Information Protection Act 1998 (NSW) ▪ Health Records and Information Privacy Act 2002 (NSW) ▪ Health Records and Information Privacy Code of Practice 2005 (NSW) ▪ Children and Young Persons (Care and Protection) Act 1998 ▪ Education and Care Services National Law ▪ Notifiable Data Breaches (NDB) scheme ▪ Freedom of Information Act 1982 ▪ Office of the Australian Information Commissioner (OAIC) ▪ Notifiable Data Breaches Scheme. ▪ Chapter 16A (Children and Young Persons (Care and Protection) Act 1998)

Contractual obligations	▪ Employment Contract ▪ Service and Support Contracts ▪ Funding Agreements

Documents related to this Policy	
Related Policies and Documents	▪ Recruitment and Onboarding Policy ▪ Code of Conduct ▪ Confidentiality Agreement ▪ Privacy Collection Statement & Consent ▪ Consent to Exchange Information Consent ▪ Media Consent Form ▪ Delegations of Authority ▪ Fraud and Corruption Policy ▪ Conflict of Interest Policy ▪ Incident Management Policy and Procedure ▪ Feedback, Complaints, Grievance and Compliment Policy ▪ Child Safety and Wellbeing policy and procedure ▪ Hazard and Incident Reporting form ▪ Feedback and Complaints form ▪ Intranet Access Form ▪ Artificial Intelligence (AI) use at Koorana Policy ▪ Acceptable use of Koorana IT Assets ▪ Use of Electronic Media Policy ▪ Cyber Security Policy ▪ Access Management Policy ▪ CCTV Policy (Preschools) ▪ Duty of Care Dignity of Risk Policy ▪ Preschool Enrolment ▪ Statement of Commitment to Child Safety

Definitions
Koorana: Koorana Child & Family Services Limited. **Client(s):** a child receiving Koorana's services, includes Parent(s)/Carer(s)/Families. **Confidential Information**: means Personal Information or Sensitive Information about Employees and Clients, includes other relevant information related to Koorana's activities **Consent**: means the informed and voluntary consent, includes implied and express consent. **Parent(s):** the parent of a client(s), includes a legal guardian and carers. **Employee:** a person employed by Koorana on a casual or permanent basis, includes Board members

Student and volunteers: a person from the community offering their talents and service to assist Koorana and employees.

Contractor(s)/Third Party(ies): a person or company that undertakes a contract to provide labour or materials or perform services.

Visitors: any individual attending a Koorana site or meeting with a Koorana representative for professional, work or client purposes.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether it is recorded in a material form or not.

Examples of personal information may include a person's name, address, contact details, date of birth, photographs or images, employment information, bank account details, tax file number, superannuation details, driver licence details and educational or academic records.

Privacy is the ability to protect personal information including being able to control who can see or use the information.

Privacy Officer: The Chief Operating Officer, or delegate as appointed.

Sensitive Information: means Personal Information that is sensitive in nature, for example, information about a person's health, sexuality, religious beliefs, criminal record, professional or trade union memberships, political opinions.

Eligible data breach: A data breach is an eligible data breach if an individual is likely to experience serious harm. The National Data Breach scheme requires regulated entities to notify individuals and the Commissioner of 'eligible data breaches'.

Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

Serious harm in the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

1. POLICY STATEMENT

Koorana is committed to protecting the rights to dignity, privacy, and confidentiality of all employees, volunteers, clients (including NDIS participants) and their families, students, contractors, and other individuals, in relation to the personal and sensitive information Koorana collects, uses, discloses and stores.

Koorana manages information in accordance with its legal, regulatory and ethical obligations and recognises privacy and confidentiality as fundamental rights. These rights are respected at all times, except where disclosure is required or authorised by law.

For the purposes of this policy, privacy refers to an individual's right to control how their personal

information is collected, used, accessed and shared. Confidentiality refers to the obligation to protect information from unauthorised access, use or disclosure.

The purpose of this Policy is to:

- Ensure employees and representatives of Koorana understand and comply with their obligations relating to privacy, confidentiality and information management.
- Provide clear and consistent processes for the lawful, ethical and secure handling of personal and sensitive information.
- Outline the rights of individuals to access, request correction of and make complaints about the handling of their personal information.
- Address the evolving information environment, including the use of digital systems and artificial intelligence, by identifying opportunities for improvement while managing associated privacy and security risks.
- Address Koorana's system for managing risks to privacy in relation to new contracts and services.

This policy is reviewed at least annually, and more frequently where required to reflect legislative change, technological developments or organisational risk. It is publicly available and can be accessed via Koorana's website.

2. PRIVACY AND CHILD SAFETY

Koorana adopts a risk-averse and child-centred approach to privacy and information management. As a Child Safe Organisation, Koorana recognises that the safety, welfare and wellbeing of children is paramount and may, in certain circumstances, override individual privacy or confidentiality considerations where required by law or to prevent harm.

Koorana protects personal information in accordance with applicable privacy legislation while ensuring compliance with mandatory reporting, child protection and other legal obligations.

Decisions relating to the collection, use or disclosure of personal information involving children are guided by the best interests of the child and duty of care approach.

All employees, volunteers, students and contractors are informed of this policy and their privacy and confidentiality obligations as part of induction or engagement with Koorana. This includes, but is not limited to, their responsibilities in relation to:

- The lawful collection, use and disclosure of personal information.
- Mandatory reporting and other statutory obligations.
- Verification and assessment of internal and external requests for information.

- Secure storage, access and handling of personal information.

As part of induction, all persons are also provided with Koorana's *Child Safety and Wellbeing Policy*, Information Technology and Cyber Security policies, and other related governance documents to ensure a consistent and integrated approach to child safety and information management

Koorana ensures that clients and, where appropriate, their families are informed about how their personal information is collected, used, stored and shared. Information about privacy and confidentiality is provided at service entry and made available throughout service delivery, including access to this policy via Koorana's website. Clients are advised of their rights to access and correct their personal information, raise concerns, and make a privacy complaint, as well as circumstances where information may be disclosed to meet child safety, mandatory reporting or other legal requirements.

Koorana appoints a dedicated Privacy Officer in accordance with this Policy to oversee compliance with privacy obligations, provide guidance to employees and manage privacy enquiries and complaints.

3. PRIVACY OFFICER

Koorana's Privacy Officer is the Chief Operating Officer, or a delegate as formally appointed.

The Privacy Officer is responsible for overseeing compliance with privacy and information management obligations, promoting strong governance and capability across Koorana and supporting employees to appropriately manage personal and sensitive information. This includes providing advice, managing privacy enquiries and complaints and responding to actual or suspected privacy breaches.

The Privacy Officer will acknowledge and respond to privacy enquiries, access requests and complaints as soon as practicable and within a reasonable timeframe, in accordance with applicable privacy legislation. Timeframes may vary depending on the nature and complexity of the request and should not exceed 28 days.

The Privacy Officer is also responsible for determining whether personal information relating to a child or young person may be disclosed to a prescribed body without the consent of a parent in accordance with Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998 (NSW)*.

3.1. Complaints and Feedback

All individuals have the right to provide feedback or make a complaint regarding Koorana's handling of personal information. Complaints or feedback may be directed to the Privacy Officer via email at privacy@koorana.org.au or as per Koorana's *Feedback, Complaints, Grievance and*

Compliment Policy.

Where a person is not satisfied with Koorana's response to a privacy concern, they may escalate the matter internally to the Chief Executive Officer. Where they are dissatisfied with that response, they may escalate externally to:

- NSW Information and Privacy Commission (for NSW privacy issues), or
- Office of the Australian Information Commissioner (for national privacy issues).

4. CONFIDENTIALITY DUTY AND USE OF INFORMATION

Koorana collects, uses and discloses personal information only for lawful and legitimate purposes related to service delivery, safety, organisational operations and regulatory compliance ("permitted uses"). Personal information will not be used or disclosed unless it is:

- Authorised by informed consent where consent is required or appropriate (e.g., signed Consent to Exchange Information Form)
- Required by law (such as but not limited to, child safety or wellbeing concerns or under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*)
- Ordered by a court or other authority.

Employees must keep confidential all employee, client and any other personal or sensitive information obtained in the course of their employment with Koorana. This duty of confidentiality commences at the start of employment, includes the signing of a Confidentiality Agreement, and continues after the termination of employment.

Employees must:

- Not access, use or disclose personal or confidential information unless authorised and necessary for permitted purposes.
- Not disclose information without consent unless permitted or required by law.
- Ensure confidential information is not left unattended, visible or stored in an unsecured manner.
- Not allow unauthorised third-parties to access confidential information.
- Immediately notify their manager and the Privacy Officer of any actual or suspected loss, unauthorised access, misuse or breach of information (refer to Section 11: Data Breach Management).

Where there is uncertainty about whether information can be accessed or disclosed, employees must seek advice from their manager or the Privacy Officer before taking action.

Any breach to the confidentiality or misuse of information may result in disciplinary action under Koorana's Performance Management Policy, and in some cases, legal consequences. See section 11. Breaches.

5. COLLECTION OF INFORMATION

Koorana collects personal information only where it is reasonably necessary to provide services, employ staff, and meet legal, contractual, or funding requirements. Information collected is relevant, proportionate and handled in accordance with this policy.

Personal information collected by Koorana may include, but is not limited to:

- Client enrolment and service information
- Employment and recruitment records
- Incident, risk and safeguarding records
- Feedback and complaints
- Quality improvement and evaluation data
- Statutory, regulatory and funding reports

5.1 Client Information

Koorana collects personal information from clients to deliver safe, effective, and lawful services. Where required, consent is sought prior to the collection, and clients (or parents/guardians for children) are provided with Koorana's *Privacy Collection Statement*, which explains:

- The type of information collected
- The purpose for which it is collected
- How the information is stored and protected
- How the information can be accessed or corrected
- The consent provided, including any limits or conditions.

Refusing consent will not disadvantage clients; however, it may limit Koorana's ability to deliver some services or meet certain legal obligations.

Preschools

For children enrolled in Koorana preschools, personal information is collected through the enrolment process and associated Privacy Collection Statement. This includes information necessary to meet education and care regulations, child safety obligations and funding requirements.

Early Intervention and Allied Health (EIAH)

For clients accessing Early Intervention and Allied Health services, personal information is

collected through service intake processes, including the Consent to Release or Exchange Information Form and the Privacy Collection Statement. This enables service delivery, referrals and compliance with NDIS and other funding obligations.

Waitlists

When joining a waitlist, clients may provide personal information such as contact details and service preferences to allow Koorana to communicate with them and assess service suitability. By providing this information, clients provide implied consent for collection and use for waitlist management purposes only, in accordance with this policy.

Start Strong Pathways (SSP) and Supported Playgroups (SPG)

For children attending Start Strong Pathways and Supported Playgroups, information is collected to ensure the safety, wellbeing, inclusion and participation. This may include health; developmental and family information provided during enrolment or registration. Consent is sought prior to collection or sharing personal information, except where disclosure is required or authorised by law, including mandatory reporting obligations.

5.2. Recruitment, Employee, Student, Volunteer and Contractor Information

Koorana collects personal information from job applicants, employees, students, volunteers and contractors for the purpose of recruitment, employment, workforce management and compliance with workplace laws and obligations. Only information relevant to employment or prospective employment is collected. This includes:

- Information required to assess applications, such as contact details, employment history, qualifications, references and right-to-work documentation.
- Secure handling of applicant information, accessible only to individuals directly involved in recruitment or for legitimate business purposes.
- Inclusion of recruitment records in the employee's personnel file for successful applicants.

The relevant Executive Leadership Team member, manager or team leader and the People & Quality team are responsible for ensuring employee and recruitment information is stored securely and accessed appropriately. All recruitment and employment information is managed in accordance with this policy, Koorana's Code of Conduct, Recruitment and Onboarding Policy, and other relevant policies. Information is not shared with external parties or used for any other purposes unless required or authorised by law. Information is stored securely in Koorana's third party systems and/or Koorana's secure environment with controls to limit access as required for business roles.

5.3 *Business-related Information*

Koorana may collect personal information from contractors, business associates, partners and through business dealings and standard operations. This may include names, emails or other personal information. All information is stored in Koorana's secure environment or third-party platforms as relevant.

6. EXTERNAL REQUESTS FOR ACCESS TO INFORMATION (INCLUDING CHAPTER 16A)

Koorana may receive external requests for access to client, employee or other personal information. All external requests are managed in accordance with applicable privacy legislation, statutory obligations and Koorana's duty of care, including its commitment to child safety. Personal or sensitive information will only be disclosed where there is a lawful basis to do so and only to the extent necessary for the permitted purpose.

External requests may include, but are not limited to:

- **Health professionals and service providers**

  Information necessary for the ongoing care or support of a client may be disclosed with a valid signed *Consent to Release/Exchange Information Form.* For children, consent must be provided by a parent or legal guardian. For children enrolled in Koorana preschools, consent may be provided through the Enrolment form.

- **Statutory and regulatory obligations**

  Personal information may be disclosed without consent where required or authorised by law. This includes mandatory reporting obligations, subpoenas or court orders, lawful requests from police, the NDIS Quality and Safeguards Commission, SafeWork NSW, or information sharing under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998 (NSW)where information relates to the safety, welfare, or wellbeing of a child or young person.

- **Employees, students, volunteers, and contractors**

  Personal or sensitive information relating to employees, students, volunteers or contractors will only be disclosed with valid consent, consent, unless disclosure is required or authorised by law, including in response to subpoenas, court orders or lawful requests from regulators.

Where consent is not provided, unclear or disputed, the matter must be escalated to the Privacy Officer before any information is disclosed. The Privacy Officer is responsible for determining whether disclosure is lawful, necessary and proportionate and for managing any associated risks or concerns.

6.1 Verification of Requests

Before any personal or sensitive information is disclosed, the identity, authority and legitimacy of the requestor must be verified.

Employee's must confirm

- The identity of the requester
- The requester's contact details, including name and official phone number
- The requester's authority to request and receive the information
- The authenticity of the request, including by returning the call via an official contact point where appropriate.

No information is to be released unless these verification steps are completed.

6.2 Legal Advice

Independent legal advice will be sought where required, including where:

- The legality of the request is unclear.
- The scope of information requested appears excessive. Or;
- There is potential risk to a child, client, staff member or the organisation.

7. RECORD STORAGE, ARCHIVING AND DESTRUCTION

7.1. Record storage

Koorana securely stores all records containing personal or sensitive information and takes reasonable steps to protect information from loss, misuse, unauthorised access, modification or disclosure. This includes the usage of the Microsoft environment and third-party platforms and applications (e.g., client information management systems, customer reference managers, employment, financial systems), with security matrixes, password protection and other security features to limit access to records only as required by role within the business.

- **Client records**

  Hard copy records are stored in locked storage with restricted access. Electronic records are stored in Koorana's approved systems and Microsoft environment which utilise industry-recognised security and access controls.

- **Applicant, Employee, Student, Volunteer and Contractor records**

  Only information relevant to employment or prospective employment is collected and retained. Employee records are stored in Koorana's employee information system (currently Employment Hero) and/or Koorana's document management platforms with appropriate security controls and access restrictions.

- **Business-related information**

  Personal information collected through business operations will be stored in Koorana's Microsoft environment or approved third-party platforms and applications.

- **Preschool CCTV footage**

  CCTV recordings are stored securely, and access is restricted to authorised personnel. Footage is generally retained for a minimum of 30 days and may be retained for longer periods where required for investigations, incidents, complaints or legal proceedings, in accordance with this policy, Koorana's *CCTV Policy*, and *Use of Electronic Media Policy*.

- **Marketing images and footage:**

  Approved marketing images and materials are stored securely via Koorana's Microsoft environment and/or approved systems or devices.

- **Images and video footage on Koorana-issued devices**

  Images and videos must only be captured and stored on Koorana-issued devices and approved applications except where exceptions are approved (e.g., at events where a private photographer is hired) by the individual and/or parent/guardian.

  Transfers to personal or non-Koorana-issued devices, USBs or unapproved cloud platforms is strictly prohibited.

  All Koorana-issued devices are password-protected and managed through Mobile Device Management (MDM). Where there is an allegation, investigation or data breach risk, Koorana may remotely lock devices via MDM until the matter is resolved.

7.2. Archiving and destruction

7.2.1. Client and Employee, Student, Volunteer and Contractor Records

Koorana adopts a conservative approach to record retention. In line with the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse, all client and employee records are retained for a minimum of 45 years, where appliable, to support delayed disclosures, investigations and legal processes. This retention period exceeds minimum requirements under the State Records Act 1998 (NSW), NDIS Practice Standards and ACECQA obligations.

Records are archived securely and access remains restricted to authorised personnel.

The destruction of records must:

- be authorised in accordance with Koorana's *Delegations of Authority Policy*; and
- comply with applicable legislative and regulatory requirements, including the State Records Act 1998 (NSW).

Unsuccessful job applications may be retained for up to 12 months for future opportunities unless the applicant requests earlier deletion.

7.2.2. Images and videos on Koorana Issued devices

Images and videos on Koorana-issued Android devices are automatically deleted after 90 days via Mobile Device Management (MDM).

On Koorana-issued iOS devices (e.g. iPads), where automated deletion is not available, staff must review and securely delete files within the 90-day period. Quarterly reminders are issued to staff to support compliance.

Retention beyond 90 days may only occur where the material is required to support an ongoing therapeutic, educational, marketing, business or legal purpose and must be approved by the relevant manager and documented.

No client-related records or images/videos should be stored on personal devices unless an exception has been approved by the individual and/or their parent/guardian (e.g., external photographer).

7.3. Recordings of Meetings

Koorana may record meetings for legitimate business purposes, including but not limited to training, supervision, quality improvement, clinical collaboration, and organisational governance. Meetings will only be recorded where participants have been informed, and where required, consent has been obtained.

Recorded meetings may include audio and/or visual information and may contain personal, sensitive or confidential information. As such, recordings must:

- Be stored securely on Koorana's approved document management system.
- Have access restricted to authorised personnel
- Be retained only for as long as necessary for the purpose for which they were created.
- Not be stored on personal devices or unapproved platforms.

Where a meeting recording is no longer required for its original purpose, it must be securely deleted in accordance with this policy.

When participating in meetings with external parties, employees must be alert to whether the meeting is being recorded or whether third-party notetaking, transcription or artificial intelligence applications are in use. Employees must not disclose personal, sensitive or confidential information in circumstances where Koorana does not control the recording, storage, access or retention of that information. Where there is uncertainty about how

meeting content will be recorded, stored or used by a third party, discussion must be limited to non-identifiable and non-confidential information, or the meeting must be paused until appropriate safeguards are confirmed. Employees are required to seek guidance from their manager or the Privacy Officer where there is any doubt.

Unless otherwise required by law, recordings of meetings are retained in accordance with the following timeframes:

- **Clinical, therapeutic or child-related meetings** (including case discussions, supervision, multidisciplinary meetings):

  As a general rule, these meetings should not be recorded. Where a recording is made, it must be retained only until the meeting minutes are formally confirmed.
- **Staff supervision, performance or employment-related meetings**:
- As a general rule, these meetings should not be recorded. Where a recording is made, it must be retained only until the meeting minutes are formally confirmed.
- **Training and professional development sessions** (including recorded webinars):

  Recordings may be made available for later viewing via Koorana's training and / or document management platforms and retained until the content becomes outdated or superseded.
- **Operational or project meetings** (including planning, implementation or internal coordination meetings):

  Retained for up to 60 days, unless required for audit, review or ongoing project delivery.
- **Governance meetings** (including Board and Committee meetings):

  Audio or video recordings are retained only until the meeting minutes are formally confirmed, after which recordings are securely deleted, unless required for legal or investigative purposes.

Retention beyond the above timeframes may occur only where:

- the recording is required for legal, regulatory or investigative purposes; or
- the recording forms part of a client or employee record and must be retained in accordance with statutory retention requirements.

Any extended retention must be approved by the Privacy Officer and appropriately documented.

Please refer to *Artificial Intelligence (AI) use at Koorana* Policy for further information regarding meeting recordings.

8. MARKETING, COMMUNICATIONS AND USE OF IMAGES.

Koorana enforces strict controls over the collection, storage, use and retention of images and

videos of children, clients and staff. Access is limited to authorised personnel, content is stored only on approved platforms and devices, and all use must comply with Koorana's *Code of Conduct, Use of Electronic Media Policy, Acceptable Use of IT Assets Policy*, CCTV Policy, and all applicable privacy and child safety legislation.

Koorana may request to use photographs, videos, testimonials, or stories of clients, employees, students, volunteers or contractors for marketing, communications, community education and the promotion of Koorana services.

Koorana will only use these images, videos or personal stories with informed, written consent, in accordance with the NSW Child Safe Standards and relevant privacy laws.

Images may be taken in other business-related contexts and used on Koorana's social medial, website, or publications. Where these involved adults who are not clients, employees, students, volunteers or contractors, posing for the photograph or video will be taken as consent for the image to be used for this purpose. Adults in this circumstance should advise Koorana if they do not consent for the image to be used for this purpose.

Where the individual is a child, consent must be provided by a parent or legal guardian prior to use of any images in marketing or social media materials.

Consent is voluntary and refusal to provide consent will not affect access to services or supports.

By providing consent, materials may be used on Koorana's website, social media platforms, printed materials such as newsletters, brochures, reports to stakeholders or fundraising campaigns. Individuals are advised that once published online or in public materials, Koorana cannot fully control how that information may be shared, copied or reused by third parties.

All images and materials are stored securely and accessed only by authorised staff. Consent may be withdrawn at any time by contacting Koorana. Withdrawal of consent will prevent future use of the material; however, previously published materials may not be able to be removed from circulation. Further information is available in Koorana's *Use of Electronic Media Policy*.

9. ACCESS AND RIGHTS TO INFORMATION

Employees and Contractors may only access client, employee, or business information that is directly relevant and necessary to their role. Unauthorised access to, or use of, or interference with information is strictly prohibited.

Clients, employees, volunteers, students, and contractors have the right to request access to their own personal or sensitive information held by Koorana and to request correction of information where it is inaccurate, incomplete or out of date. Employees may also access business information

relevant to their role subject to access controls.

Requests for access or correction must be directed to the Privacy Officer. In responding to a request:

- Information relating to third parties may be redacted or de-identified to protect privacy.
- Requests will be handled within a reasonable timeframe in accordance with legislative requirements.
- Access will be provided at minimal or no cost, unless otherwise permitted by law.

In accordance with the Fair Work Act 2009 (Cth), employees also have the right to decide whether to disclose information about their pay and employment conditions with other employees. It is up to the individual if they wish to disclose. Koorana will not take adverse action against an employee for choosing to exercise or not exercise, this right.

10. ELECTRONIC MEDIA AND CCTV

10.1.Prohibited use of electronic devices

From 1 September 2025, enhanced child safety requirements apply in preschool environments. Personal electronic devices, including mobile phones, tablets and smart watches, must not be used by employees, students, volunteers or contractors while children are present, unless expressly authorised for work-related purposes.

This requirement supports child safety and privacy by ensuring that images, audio or recordings of children are only captured, stored and shared using Koorana-issued devices and approved applications in accordance with this policy and Koorana's *Use of Electronic Media policy*.

Any approved exceptions must be managed in line with relevant policies and documented appropriately.

10.2.CCTV in Preschools

Koorana Preschools utilise closed-circuit (CCTV) systems to support the safety and security of children, families, employees, contractors and visitors. CCTV footage may be used for risk management, incident investigation, security monitoring and evidentiary purposes where required.

CCTV systems are operated in accordance with applicable privacy and surveillance legislation, and access to footage is restricted to authorised personnel. Appropriate signage is displayed, to inform individuals that CCTV is in use.

Koorana may engage external service providers to manage or store CCTV data. Where third-party data processors are engaged, contractual safeguards are in place to ensure the security,

confidentiality and integrity of CCTV footage.

10.3.Facial Recognition Capability

Some of Koorana's CCTV and security systems have the technical capability to support facial recognition functionality. Where facial recognition technology is used, Koorana will ensure its operation complies with applicable privacy, surveillance and child safety laws. Appropriate signage will be displayed to notify individuals that CCTV and facial recognition technology are in use.
Any use of facial recognition technology must be for legitimate safety, security or operational purpose, be proportionate to the identified risk, and be subject to appropriate governance approval and documented risk and privacy assessment. Facial recognition will not be used in a manner that is inconsistent with Koorana's child safety obligations or privacy principles.

11. DATA BREACH MANAGEMENT

A data breach occurs when personal information held by Koorana is accessed, disclosed or used without authorisation, or where personal information is lost in circumstances likely to result in unauthorised access or disclosure. A data breach may trigger internal escalation and external notification obligations.

11.1.Identifying and reporting data breach

Employees must immediately report any actual or suspected data breach to their manager, who must escalate the matter to the Privacy Officer without delay.

All data breaches must be reported **immediately verbally** and followed with using Koorana's *Hazard and Incident Reporting Form* **within 24 hours** of the employee becoming aware of the breach. The assessment and response to a data breach will be managed in accordance with Koorana's *Risk Management Framework* and *Incident Management Policy and Procedure.*

All data breaches are recorded In Koorana's *Hazard and Incident Reporting Register*.

Failure to report a suspected data breach may itself be treated as a breach of this policy.

11.2.Notifiable data breach

Koorana is required under the Privacy Act 1988 (Cth) to comply with the Notifiable Data Breaches (NDB) scheme. Koorana must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) where an eligible data breach is likely to result in serious harm. Serious harm may include, but is not limited to, identify theft, financial loss, physical harm,

psychological harm or reputational harm.

An eligible data breach occurs when the following criteria are met:

- there is unauthorised access to, or disclosure of personal information held by Koorana or a contracted service provider, or the information is lost in circumstances where unauthorised access or disclosure is likely; and
- the breach is likely to result in serious harm to one or more individuals; and
- Koorana or the contracted service provider has been unable to prevent the risk of serious harm through remedial action.

Where Koorana has reasonable grounds to believe that an eligible data breach has occurred, Koorana must promptly notify the OAIC and affected individuals in accordance with legislative requirements.

If Koorana suspects that a data breach may be an eligible data breach, Koorana must complete an assessment within 30 calendar days to determine whether notification is required.

11.3.Employee Responsibilities

Employees must comply with Koorana's Acceptable Use of IT Assets and Artificial Intelligence (AI) Use Policy and take reasonable steps to prevent data breaches, including following security, access and reporting requirements.