QA7 – CONFIDENTIALITY, PRIVACY AND SECURITY PROCEDURE

INFORMATION

We understand that we receive and hold sensitive information. It is of the utmost importance to us that families, staff and the community trust us, and know that this information is treated with respect, and kept private and confidential.

We are committed to safeguarding the privacy, dignity and confidentiality of individuals. We work to ensure all records and information about individual children, families, educators and management is treated with discretion and kept in a secure place, accessible by or disclosed to only those authorised individuals who need the information to fulfil responsibilities, or who have a legal right to know.

RESPONSIBILITIES

All team members, visitors, students and volunteers must comply with this procedure.

PROCEDURE

OBLIGATIONS AND RESPONSIBILTIES

- All staff will be trained to ensure they are fully aware of and understand their obligations and responsibilities in relation to maintaining strict confidentiality under the Privacy Act (1988).
- Team members will treat confidential information with care and sensitivity and only disclose the information to those who are authorised and have a need for the information. If information is required to be shared by law, team members will comply with this requirement.
- When a team member ceases employment, all confidential information must be returned. It is expected that post-employment, confidential matters will remain confidential and will not be disclosed to another party.
- If a team member is found to have breached any confidentiality while employed with the centre, they may be disciplined, and in some cases dismissed.
- If a person is found to be in breach outside of employment with the centre, legal action may be taken depending on the severity of the breach.
- If there are any suspected breaches of security, confidentiality or privacy, team members must report it to the Centre Manager/Nominated Supervisor/Management immediately.

USE OF AND ACCESS TO INFORMATION

- Families have the right to request access to their own personal information at any time.
- Educators may need to share personal information about a family or child with another educator to ensure they can care for and support the child and family to the best of their abilities.

- Families will be informed about which people have authorised access to their child's personal information.
- If information has been shared with an external agency due to legal obligations, families will be notified as soon as possible and practicable. Depending on the reason for the information share, families may be notified by either the centre, or the external agency.

STORAGE

Confidential and/or sensitive information will be stored in a secure location and will not be left or made available in a public or shared area.

DIGITAL INFORMATION SECURITY

Authentication
To ensure information security, team members must take all reasonable steps to keep devices and information secure by:

- Having passwords enabled on all devices
- Storing devices in safe and secure locations; they are not to be left in public
- Keeping confidential information in locked, secure locations
- Not sharing passwords or information with others.

Photographs and videos

- During enrolment consent for the child to be photographed or videoed will be captured. If this consent changes at any time, it must be updated in the child's file, and all team members must be notified.
- If a child's photo or video is intended to be used for marketing purposes, a separate written approval will be sought.
- Any photos or videos of children should only be captured on centre devices, never on a team members, visitor or volunteer's personal device.
- When taking group photos/videos, team members must ensure any children who do not have consent are not visible or identifiable in the image.
- All photos or videos should be moved to the OneDrive Cloud regularly and deleted from the tablets.

NOTIFIABLE DATA BREACHES SCHEME

- We are required under The Privacy Act and the Notifiable Data Breaches (NDB) Scheme to report eligible data breaches.
- The Privacy Act requires early childhood education and care providers to take certain steps if any personal or sensitive information they hold about families and/or children, is improperly accessed, disclosed or lost; failure to do so can attract significant fines.
- Centres are required to proactively protect the personal and health related data they hold and report qualifying breaches to the Office of the Australian Information Commissioner (OAIC).

Examples of data breaches:

- A dismissed employee taking the centre emergency contact list home and spending the weekend texting parents about the centre
- Child specific medical or allergy information being on display or accessible to other parents, without written consent

- Children's data on an iPad being accessed outside of the centre or left on a train and not logged off.

If a breach occurs:

- We commit to conducting a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm, and as a result require notification
- We will work to ensure an assessment is completed within 30 days
- If an eligible data breach is confirmed, we will, as soon as practicable, provide a statement to each of the individuals whose data was breached or who are at risk, including details of the breach and recommendations of the steps they should take. A copy of the statement will also be provided to the OAIC
- We will notify individuals whose personal information is involved in a data breach where the breach is likely to result in serious harm. This notification will include recommendations about the steps they should take in response to the breach. The OAIC will be notified of the breach.
- We will lodge our statement about an eligible data breach to the OAIC through the Notifiable Data Breach statement.

ACKNOWLEDGEMENTS, REFERENCES AND RESOURCES

Australian Government – Federal Register of Legislation. (n.d.) *Privacy Act 1988.* Accessed 8 July, 2019 from https://www.legislation.gov.au/Series/C2004A03712

Office of the Australian Information Commissioner. (n.d.) *Notifiable Data Breaches Scheme.* Accessed 8 July, 2019 from https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify

DOCUMENT CONTROL

Date Reviewed	Modifications
Aug 2019	Reviewed and created new policy document
18 January 2022	No changes