PRIVACY LAW COMPLIANCE PROCEDURE

Under National Law, Section 263, Early Childhood Services are required to comply with Australian privacy law which includes the Privacy Act 1988 (the Act) aimed at protecting the privacy of individuals. Schedule 1 of the Privacy Act (1988) includes 13 Australian Privacy Principles (APPs) which all services are required to apply. The APPs set out the standards, rights and legal obligations in relation to collecting, handling, holding and accessing personal information.

The Notifiable Data Breaches (NDB) scheme requires Early Childhood Services, Family Day Care Services, and Out of School Hours Care Services to provide notice to the Office of the Australian Information Commissioner (formerly known as the Privacy Commissioner) and affected individuals of any data breaches that are 'likely' to result in 'serious harm'.

Key Points- under the Australian Privacy Act (1988) (Cth) (Privacy Act), Early Childhood Education and Care (ECEC) Service providers are required to:

- notify individuals who may be affected by a data breach or the potential exposure of their data
- notify the Office of the Australian Information Commissioner (OAIC) if a service experiences a data breach
- notify an eligible data breach where there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the Service
- prepare a data breach statement to the OAIC and take the required steps to notify the affected individuals about the contents of the data breach statement.

A failure to notify a serious interference with privacy under the Privacy Act may result in a fine of up to $420,000 for individuals and up to $2.1 million for organisations.

Working in conjunction with the *Privacy and Confidentiality Policy*, this procedure provides detailed steps on how management can manage sensitive personal information and react to data breaches.

Education and Care Services National Law or Regulations (R.168, 181 and 181-184) NQS QA 7: Element 7.1, 7.1.1, 7.1.2, 7.1.3 and 7.2 Governance practices and procedures
Related Policy: Privacy and Confidentiality Policy and Cyber Safety Policy

STEP 1: PRIVACY AND CONFIDENTIALITY POLICY		
1	Management will discuss any changes to the Australian Privacy Principles and Privacy Act 1988 with all educators and staff of the service – for example: during a team meeting or staff notification	
2	Management will review and update the service's *Privacy and Confidentiality Policy*. Gather information and feedback from stakeholders, including staff, families and management	
3	Management will review contracts with software providers to ensure they have adequately addressed the privacy law changes to maintain compliance within the service	

STEP 2: PRIVACY AUDIT		
1	It is recommended that management conduct a *Privacy Audit* to ensure ongoing compliance with privacy obligations and recent changes. The Privacy Audit should be completed on a yearly basis or following any breaches in data at the service. The Privacy Audit will assist Services to: - Identify how to meet privacy obligations - Identify how to improve on existing privacy management - Identify potential areas of privacy risk - - Alleviate these risks by improving compliance with the Privacy Act	
2	To ensure compliance, Services must review all contracts with software providers to ensure they have adequately addressed the privacy law changes. This includes Child Care Software (CCS) management programs and Early Childhood Documentation Software programs.	

STEP 3: DISCUSSING PRIVACY CHANGES		
1	It is vital to discuss Privacy Law changes with the service team outlining the privacy principles that outline standards that must be met regarding the collection, use, disclosure and storage of personal information.	
2	Using research conducted and feedback gained from stakeholders; update Privacy and Confidentiality Policy ensuring compliance with Privacy law.	

STEP 4: UPDATE SERVICE'S COLLECTION STATEMENT		
1	APP 5 requires entities that collect personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters, which include: - The APP entity's identity and contact details - The fact and circumstances of collection - Whether the collection is required or authorised by law - The purposes of collection - The consequences if personal information is not collected - The entity's usual disclosure of personal information of the kind collected by the entity - Information about the entity's APP Privacy Policy	

	- - Whether the entity is likely to disclosure personal information to overseas recipients, and if practicable, the countries where they are located	

STEP 5: DATA BREACH RESPONSE PLAN		
1	Services are required to have a *Data Breach Response Plan* which sets out procedures in the event of a data breach (or suspected data breach). A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.	
2	A *Data Breach Response Plan* will enable management to contain, evaluate the risks, consider the breach and review and respond to a data breach.	

PRIVACY COLLECTION STATEMENT - EXAMPLE		
1	Our Service [Insert Name] will not use personal information for any purpose that is not reasonably required for the appropriate or effective operation of the Service. The privacy of all information provided is paramount which we as a Service will protect at all times. Personal information gathered by the Service may be accessed by and exchanged with staff educating and caring for a child, by administrative staff or for legal requirements. Personal information collected may include, medical information, income and financial details, contact information, children's developmental records, legal information, employment/martial information, qualifications, staff entitlements, and information required under the National Law and Regulations. We may disclose personal information where we are permitted or obligated to do by Australian law. This may include - Government employees - Authorised officers during Assessment and Rating - Software companies that provide computer based educational programs which use children's personal - information - Lawyers in relation to a legal claim - Debt collection agency where fees are outstanding - Officers carrying out an external dispute resolution process - Protecting individuals from serious misconduct or to prevent a serious threat to a life, health or safety. Personal information is stored in a safe and secure manner, using locked filing cabinets or password protected database and computer. Information is backed up electronically and stored securely. Hard copy information is stored securely at the Service and archived in accordance with regulatory requirements when no longer needed.	

	Our Service will gather written permission prior to disclosing personal information. This may include, displaying medical plans or early intervention services. We are committed to safeguarding and protecting the privacy of personal information and adhere to the Australian Privacy Principles. By providing our service with personal information, you consent to the collection, storage and use of personal information in the ways described in our policy and collection statement.	

DATA BREACH RESPONSE PLAN		
1	Contain the breach and do a preliminary assessment - Identity the breach or suspected breach - Immediately contain breach - Preserve evidence that may be used in determining the cause of the breach	
2	Assess-evaluate the risks for individuals associated with the breach Conduct initial investigation and collect information about the breach, including: 1. Date, time, duration and location of the breach 2. The personal information breached 3. Details about how the breach was discovered and by whom 4. Establish the cause and extent of the breach 5. Details of the affected or possibly affected individuals 6. Assess the risk of harm to the affected person/s 7. Assess the risk of other harms (legal liability, reputational damage etc.) - Determine if the context of information is important - Establish the source and level of the breach - Assess priorities and risks based on what is known - Keep appropriate records of the suspected breach and action of the response team, including steps taken to rectify the situation and the decision made	
3	Notify- consider breach notification - Determine who needs to be made aware of the breach - Determine the requirement to notify the affected individual/s - Consider whether others need to be notified, including law enforcement, agenises, OAIC etc. - Notifications should be direct to the affected individual/s Notification information should include: 1. Incident description 2. Type of information involved 3. Response to the breach 4. Assistance offered to the affected person 5. Detailed information to assist in privacy protection 6. Service contact details	

	7. If the breach has been notified to external contacts (Police, insurance providers, regulatory bodies etc.) 8. Legal implications 9. How individual/s can lodge a compliance with the Service 10. How individuals can lodge a complaint with the OAIC	
4	**Review the incident and act to prevent future breaches** - Investigate the cause of the breach in its entirety - Report the outcome to the OAIC - Make appropriate changes to policies and procedures (if required) - Review staff training practices (if required)	

The template above is a guide only and services must edit to reflect practices that are accurate and relevant to their context, statement of philosophy and physical environment.