DATA BREACH RESPONSE PROCEDURE

Data breaches must be dealt with on an individual basis, by assessing the risk to elect the appropriate course of action. There are 4 steps to consider when responding to a breach or a suspected breach of privacy.

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.

Working in conjunction with the *Privacy and Confidentiality Policy*, this procedure provides detailed steps for management to follow to contain, evaluate the risks, consider the breach and review and respond to a data breach.

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

DATA BREACH RESPONSE		
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.	

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	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	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. 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)	