Data Breach Response Checklist

STEP 1

Contain the breach and make a preliminary assessment

☐	Convene a meeting of the data breach Response Team.
☐	Immediately contain breach: o IT to implement the ICT Incident response plan if necessary o Building security to be alerted if necessary
☐	Inform the Executive Team, provide ongoing updates on key developments.
☐	Ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing Approach Services to take appropriate corrective action.
☐	Consider developing a communications or media strategy to manage public expectations or media interest.

STEP 2

Evaluate the risks for individuals associated with the breach

☐	Conduct initial investigation, and collect information about the breach promptly, including: o the date, time, duration and location of the breach o the type of personal information involved in the breach o how the breach was discovered and by whom o the cause and extent of the breach o a list of the affected individuals, or possible affected individuals o the risk of serious harm to the affected individuals o the risk of other harms
☐	Determine whether the content of the information is important.
☐	Establish the cause and extent of the breach.
☐	Assess priorities and risks based on what is known.
☐	Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.

STEP 3

Consider breach notification

☐	Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage.
☐	Determine whether to notify affected individuals – is there a *real risk of serious harm to the affected individuals?*
☐	Consider whether others need to be notified, including police, Australian Privacy Commissioner, or other agencies or organisations affected by the breach, or where Approach Services is contractually required or required under the terms of an MOU to notify specific parties.

STEP 4

Review the incident and take action to prevent future breaches

☐	Thoroughly investigate the cause of the breach.
☐	Report to Executive Team on outcomes and recommendations: o update security and response plan if necessary o make appropriate changes to policies and procedures if necessary o revise staff training practices if necessary o consider the option of an audit to ensure necessary outcomes are affected