Notifiable Data Breach Procedure

1. Purpose

This procedure provides the process for recognising, assessing and responding to a data breach within the Department for Child Protection (DCP). This procedure incorporates all data breaches that occur containing personal information and steps to follow to assess and remediate breaches. This also includes the required additional steps to notify Office of the Australian Information Commissioner (OIAC) if the data breach contains Commonwealth generated information such as a Tax File Number (TFN).

2. Scope

This procedure applies to all employees, volunteers, students, contractors and consultants providing services or products to DCP. It applies to assessment of data breaches and determining appropriate action regarding response and notification.

3. Authority

3.1 Legislative context

The Notifiable Data Breaches scheme was introduced by an amendment to the Commonwealth *Privacy Act 1988* on 22 February 2017. The Notifiable Data Breaches scheme requires any specified organisation or agency (including DCP) to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

3.2 Whole of Government requirements

The Premier and Cabinet circular, PC012 Information Privacy Principles Instructions (IPPI) defines the principles for state government agencies and third parties engaged by government, for collecting, storing, accessing, correcting, using and disclosing personal information they are responsible for.

The Privacy Committee of South Australia (PCSA) is responsible for monitoring the implementation of the IPPI.

The Premier and Cabinet circular, PC042 Cyber Security Incident Management addresses the requirements for Agencies to report, manage and respond to cyber security incidents in coordination with DPC's Control Agency for Cyber Crisis.

The South Australian Cyber Security Framework (SACSF) policy statements:

1.1 Leadership		2.6 Robust ICT Systems and Operations	☑
1.2 Organisational Structure and Staff Responsibilities		2.7 Vulnerability Management	
1.3 Risk Management	☑	2.8 Network Communications	
1.4 Policies, Procedures and Compliance	☑	2.9 System and Software Acquisition	
1.5 Supplier Management	☑	2.10 Secure Software Development	
1.6 Audit and Assurance		2.11 Cloud Computing	☑

2.1 Information Asset Identification and Classification		2.12 Mobile Device Management	
2.2 Incident Management	☑	2.13 Teleworking	
2.3 Resilience and Service Continuity		3.1 Personnel Security Lifecycle	
2.4 Access to Information		4.1 Physical Security	
2.5 Administrative Access			

3.3 DCP requirements

The Information Governance and Systems Policy should be read in conjunction with this procedure. The Information Governance and Systems Policy states that all users are required to preserve the confidentiality and privacy of the departmental information that they access.

The Significant incident reporting procedure should also be read in conjunction with this procedure. The Significant incident reporting procedure states that a data breach is a reportable significant incident and a significant incident report must be completed.

4. Procedure requirements

4.1 Data breach considerations

The Privacy Act defines a data breach as unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information. A data breach is considered to have occurred when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or heightened by a variety of factors, impact different types of personal information and create a range of actual or potential harm to individuals, agencies and organisations.

The key point to consider when determining if a data breach has occurred is regarding the concept of serious harm. 'Serious harm' is not defined in the Privacy Act or the IPPI, but OAIC suggests in the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. It is also important to consider the likelihood of serious harm to an individual as a result of the data breach. For example, unauthorised release of personal information related to children and young people in care may allow their location to be determined, which could have a significant impact to their safety. This will determine if the data breach is eligible for a mandated response, under the DPC Guideline, or if minor in nature requiring a standard response (see Appendix 1). The likelihood of serious harm is defined as harm being more probable than not.

A data breach can be defined as follows:

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

  For example, an employee browses sensitive client records without any legitimate purpose, or a computer network is compromised by an external attacker resulting in personal information being accessed without authority.

- **Unauthorised disclosure** occurs when DCP, whether intentionally or unintentionally, makes personal information accessible or visible to others outside DCP, 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 DCP.

For example, an employee of DCP accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet.

- **Loss** refers to the accidental or inadvertent loss of personal information held by DCP, in circumstances where is it is likely to result in unauthorised access or disclosure.

  An example is where an employee of DCP leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.

Under the Commonwealth Notifiable Data Breach (NDB) scheme, if Commonwealth generated personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach. However, entities that collect and hold specific Commonwealth generated information are required to notify the OAIC when a data breach occurs that may cause serious harm to the individuals affected.

Note: All reasonable steps are to be taken to complete an assessment of a suspected or confirmed data breach within 30 calendar days of when the discovery of the suspected data breach occurred. If the assessment cannot be completed in 30 days, documentation must be prepared to show that all reasonable steps were taken and the reasons for the delay.

4.2 Identify data breach response stakeholders

If a data breach is classified as minor (that there is low risk of serious harm to an individual based on the breach), then it is at the discretion of the director who was notified of the breach to determine if a Data Breach Response Team should be formed.

In the event of a breach that is determined to present a high risk of serious harm to an individual or group of individuals, a Data Breach Response Team should be immediately convened consisting of:

ICT and Information Management		**Service Delivery and Practice**	**Legal Services**	**Media and Communications**	**HR**	**Audit and Risk**
Chief Information Officer	Manager, Information Governance	Deputy Chief Executive	Director, Legal Services	Media and Digital Manager	Group Manager, Employee Relations	Manager, Audit and Risk

The Data Breach Coordinator is primarily the Chief Information Officer or delegate. A high-level diagrammatic view of the coordinator process is shown in Appendix 2.

4.3 Determine if a data breach has occurred

A data breach has occurred when the following three criteria are confirmed:

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation holds.
2. This is likely to result in serious harm to one or more individuals.
3. The organisation has not been able to prevent the likely risk of serious harm with remedial action.

There is no single method of responding to a data breach. Data breaches must be managed on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected breach.

- **STEP 1**: Contain the breach and make an assessment.
- **STEP 2**: Evaluate the risk to individuals impacted by the breach.
- **STEP 3**: Notification of breach to individuals.
- **STEP 4:** Lessons learned to prevent future data breaches.

The Data Breach Response Team (refer to Section 4.2) should perform steps 1, 2 and 3 either simultaneously or in quick succession. Appendix 3 provides a list of potential tasks to guide the actions of the Data Breach Response Team.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

Refer to Appendix 1 for a schematic overview of the process.

4.3.1 Responding to a data breach

Step	Description	Responsibility
Data breach occurs or is suspected	Refer to: DCP Data Breach Notification Process Overview DCP staff identifies/is informed of the data breach or suspected data breach and alerts their line manager immediately, noting priority escalation to director is required immediately. DCP staff member should record the time and date the breach/suspected breach was discovered, the type of personal information involved, the cause and extent of the breach and the context of the affected information. A rapid assessment is critical in providing an effective response to a data breach. The director of the business unit should initially be contacted via telephone (or face-to-face if easily done) to lead the initial assessment. Follow up should be in writing. The director should have sufficient authority to conduct the initial investigation, gather any necessary information and make initial recommendations. If necessary, a more detailed evaluation may subsequently be required. Some data breaches may be comparatively minor, and able to be managed easily without action from the Data Breach Coordinator. For example, a DCP staff member may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue to the Data Breach Coordinator. A confirmed or suspected data breach requires escalation to the Data Breach Coordinator for review and input into the assessment. In referring a breach to the Data Breach Coordinator for review, directors should consider the following questions: • Are multiple individuals affected by the breach or suspected breach? • Is the data notifiable under the Act? • Is there (or may there be) a real risk of serious harm to the affected individual(s)? • Does the breach or suspected breach indicate a systemic problem in DCP processes or procedures? • Could there be media or stakeholder attention as a result of the breach or suspected breach? If the answer to any of these questions is 'yes', then it is appropriate for the director to notify the Data Breach Coordinator. If in doubt, speak to the Data Breach Coordinator.	DCP staff alerts their line manager immediately, noting priority escalation to director is required immediately.

	For all data breaches, please contact ICT&IM Security via the ICT Service Desk on [redacted] who will provide and assist with the completion of a Security Incident Report Form.	
Step 1	Refer to: • DCP Data Breach Response Checklist The director determines: 1) Whether a data breach has or may have occurred. 2) Whether the data breach involves notifiable data, or is serious enough to escalate to the Data Breach Coordinator. 3) If so, immediately escalate to the Data Breach Coordinator. 4) If the breach can be managed at the director level, the director must send a brief email to Data Breach Coordinator advising of the situation. The director then **contains the breach and makes an assessment.** Take immediate action to contain the breach. This includes things like disabling access to electronic information or restricting physical access to paper based information. Where DCP staff are involved, the Group Manager, Employee Relations within Human Resources should be notified of the data breach.	DCP director
Step 2	*In cases where there is risk of serious harm, the director escalates to Data Breach Coordinator. Refer to* Data Breach Coordinator (DBC) process. The director, **evaluates the risk to individuals impacted by the breach** and determines whether there is a need to assemble a team that could include representatives from appropriate parts of the agency. Consider the following preliminary questions: • What personal information does the breach involve? • What was the cause of the breach? • What is the extent of the breach? • What are the harms (to affected individuals) that could potentially be caused by the breach? • How can the breach be contained? • Was the data breach of Notifiable Data Breach under the Privacy Act? (see the "Data breach occurs or is suspected" section above for guidance on determining this). To determine what other steps are immediately necessary, the risks associated with the breach should also be considered, including: • The type of personal information involved. ○ Was the information breached that of a sensitive and identifiable nature? Examples include tax file numbers and residential addresses.	DCP director and DCP Data Breach Coordinator (in cases where there is risk of serious harm)

	• The context of the affected information and the breach.
	  ○ Are there any other conclusions that can be gained from the information breached?
	• The cause and extent of the breach.
	  ○ Was it electronic or a paper/physical access related breach?
	  ○ Does it present a physical or information security issue?
	  ○ Understanding this will assist in determining who to involve in the Data Breach Response Team.
	• The risk of serious harm to the affected individuals.
	  ○ Is there a real risk of serious injury to individuals as a direct result of the breach?
	• The risk of other harms.
	  ○ Are there risks to individuals that can be identified to data contained in the breach? Does this create a serious harm risk?
	
	An assessment of the risk of harm to individuals that the information relates to will also determine the severity of the breach. Examples of harm to individuals from a data breach include:
	• identity theft
	• financial loss
	• threat to physical safety
	• threat to emotional wellbeing
	• loss of business or employment opportunities
	• humiliation, damage to reputation or relationships
	• workplace or social bullying or marginalisation.
	
	Are there any other risks to individuals or the organisation, including:
	• loss of public trust in the agency, government program, or organisation
	• reputational damage
	• loss of assets (for example, stolen computers or storage devices)
	• financial exposure (for example, if bank account details are compromised)
	• regulatory penalties (for example, for breaches of the Privacy Act)
	• extortion
	• legal liability
	• breach of secrecy provisions in applicable legislation.
	---------- 	
	In cases where there is risk of serious harm, the Data Breach Coordinator will form the Data Breach Response Team which consists of representatives from:
	1) Service Delivery and Practice
	2) ICT and Information Management
	3) Legal Services	

	4) Media and Communications 5) Audit and Risk. If the information breached includes or is suspected to include information that could in any way harm children or young people, a significant incident report must also be completed, and will be coordinated by the Data Breach Coordinator.	
Step 3	*Proceed with Step 3 only where there is risk of serious harm. Otherwise go to Step 4.* The Data Breach Response team in consultation with Data Breach Coordinator determine who needs to be notified. **Notification of breach - individuals, PCSA and OAIC** Determine who needs to be made aware of the breach (internally, and potentially externally). Individuals In some cases, it may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals). Prompt notification to individuals in these cases can help mitigate the damage by taking steps to protect themselves. Consideration should be given to when and how to notify the individuals (in writing, by telephone or in person) and who should make the notification. Consider what information should be included in the notification and if any other parties should be notified. Notification is an important mitigation strategy for both individuals and DCP. However, while notification is highly effective in responding to and managing a breach, it may not always be the most appropriate way to respond. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notification. Each breach needs to be considered on a case-by-case basis to determine whether breach notification is required. Notifications internal to DCP Escalate the matter internally as appropriate, including informing the director, the Data Breach Coordinator and Significant Incident Reporting Unit. It may also be appropriate to report such breaches to relevant internal investigation units, such as the Audit and Risk team. Privacy Committee of South Australia (PCSA) In line with the DPC Personal Data Breaches Guideline the Privacy Committee of South Australia should be notified.	Data Breach Response Team Data Breach Coordinator

	Notifications to other bodies: The Data Breach Response Team must also report the matter to the Office for Public Integrity (OPI) if it is reasonably suspected a South Australian public officer has broken the law or acted in a way that is seriously inappropriate or negligent. The OPI may refer complaints to the Ombudsman SA and the Independent Commission Against Corruption. Consider developing a communications or media strategy to manage public expectations and media interest. Office of the Australian Information Commissioner (OAIC) The notification to OAIC can be done by completing the Notifiable Data Breach Form and will be coordinated by the Data Breach Coordinator.	
Step 4	The director or the Data Breach Response Team reviews preventative measures and data breach response plan for any improvements. **Lessons learnt to prevent further data breaches** Once the data breach has been contained, impacted individuals notified and the cause of the breach rectified, a review of the response to the data breach should be conducted. This review should include: • a security audit of both physical and technical security • a review of related policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies) • a review of employee selection and training practices • a review of service delivery partners (for example, offsite data storage providers).	Director or Data Breach Response Team

4.4 Communications plan

The handling of communication and transparency is a key factor in successfully addressing and managing a suspected or confirmed data breach.

If there has been a suspected or confirmed data breach of personal information, the *owner(s)* of that information should be notified via telephone or in writing by the DCP business data owner of the following:

- the identity and DCP contact details
- a description of the data breach
- the kind(s) of information involved in the data breach and
- recommended steps individuals should take in response to the data breach as soon as practical*.

If direct contact and notification to individuals of a suspected or confirmed data breach cannot be made, DCP should consider publishing a statement on its website or social media and may need to provide details as per the dot points in this section 4.4.

Notification of data breaches to the *Privacy Committee of South Australia* should be facilitated by the Data Breach Coordinator and include:

- The action taken to ensure that the Principles as per the IPPI are implemented, maintained and observed in the agency for which he or she is responsible.
- The name and designation of each officer with authority to ensure that the Principles are so implemented, maintained and observed.
- The result of any investigation and report, under Clause 8 of the IPPI, in relation to the agency for which they are responsible and, where applicable, any remedial action taken or proposed to be taken in consequence.

Notification of data breaches to the *Office of the Australian Information Commissioner* (OAIC) should be facilitated by the Data Breach Coordinator and can be done by completing the Notifiable Data Breach Form.

If a director decides not to escalate a minor data breach or suspected data breach to the Data Breach Coordinator for further action, the director should:

- Send a brief email to the Data Breach Coordinator that contains all of the following information:
    - Description of the breach or suspected breach.
    - Action taken by the director or DCP staff member to address the breach or suspected breach.
    - The outcome of that action.
    - The director's view that no further action is required.
- Save a copy of that email in the appropriate Digital Workspace file. The Data Breach Coordinator is responsible for ensuring that a secure Digital Workspace file exists and all correspondence relating to the breach is stored in this file. Each data breach instance should be a separate file within the Digital Workspace.

* Practicable is defined as the most immediate and appropriate time since the data breach was discovered.

5. Compliance, monitoring and evaluation

- Review of this procedure will occur biennially as per SACSF Section 1.4 for Tier 2 departments.
- A mock scenario will be developed and the plan will be used to respond to the scenario to test the plan's effectiveness and ease of use.
- The Chief Information Officer is responsible for conducting the review and scenario development.
- A briefing on the outcome of the scenario will be provided to the Technical and Information Governance Subcommittee and to the Senior Executive Group.

6. Related documents

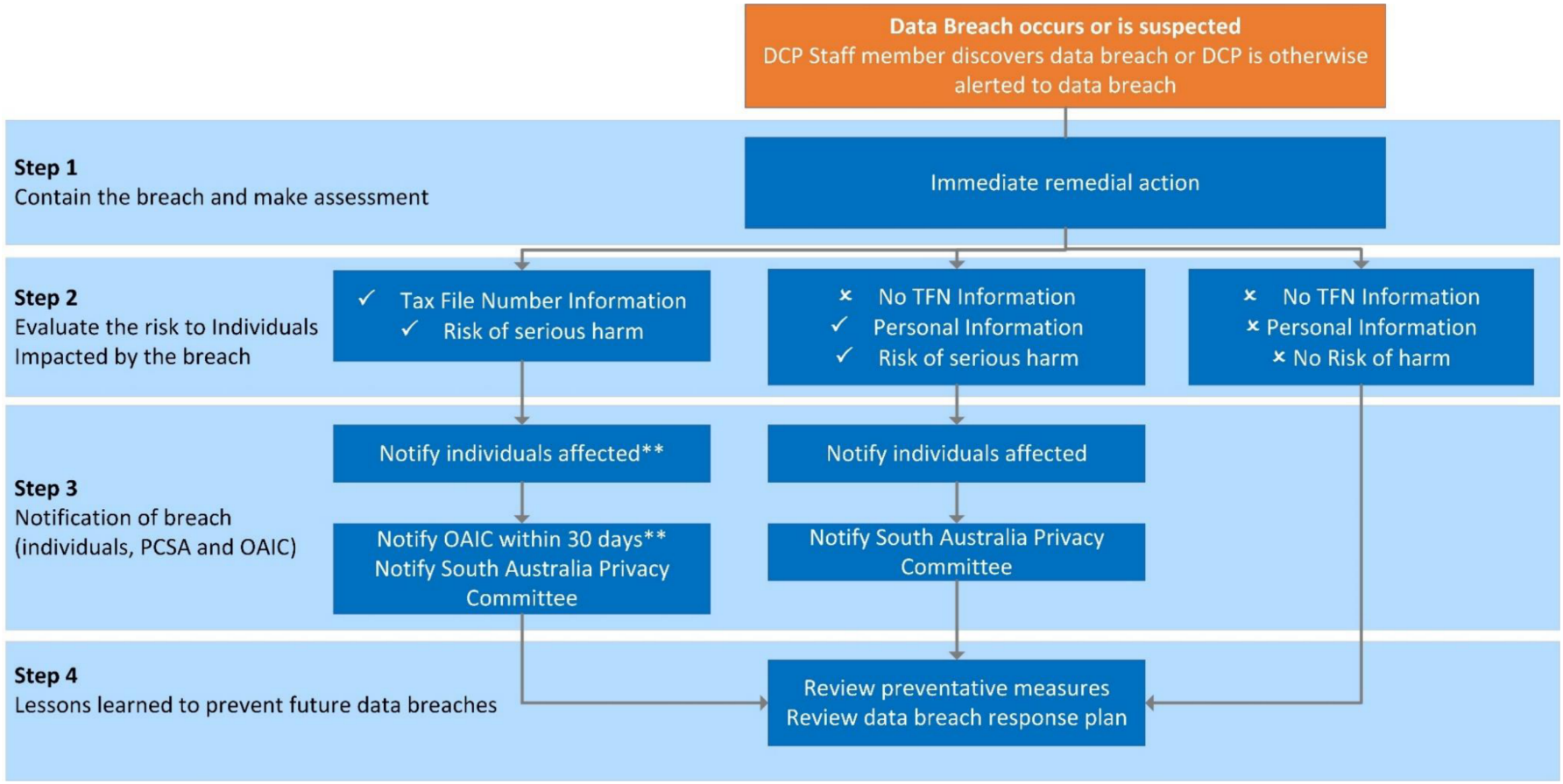
Related documents, forms and templates	
Form	Office of the Australian Information Commissioner (OAIC) – Notifiable Data Breach form for use when notifying the OAIC of a serious data breach
Scheme	Office of the Australian Information Commissioner (OAIC) for information about the Notifiable Data Breach scheme.
Instructions	PC012 – SA Government Information Privacy Principles Instruction PC042 - Cyber Security Incident Management found in Premier and Cabinet Circulars
Act	The Privacy Act 1988 and Australian Government Privacy Amendment (Notifiable Data Breaches) Act 2017
Cyber Security Framework and related documents	The South Australian Cyber Security Framework (SACSF) SACSF G4.0 Guideline on Cyber security incident reporting

Document control

Reference No./ File No.			
Document Owner		**Lead Writer (name, position)**	
Directorate/Unit: ICT & Information Management Chief Information Officer: Matthew Hawkins		Peter Vasilopoulos, Principal Security Advisor	
Commencement date	1 April 2022	**Review date**	1 April 2025
Risk rating Risk Assessment Matrix	**Consequence Rating**	**Likelihood**	**Risk Rating**
	Moderate	Unlikely	Moderate

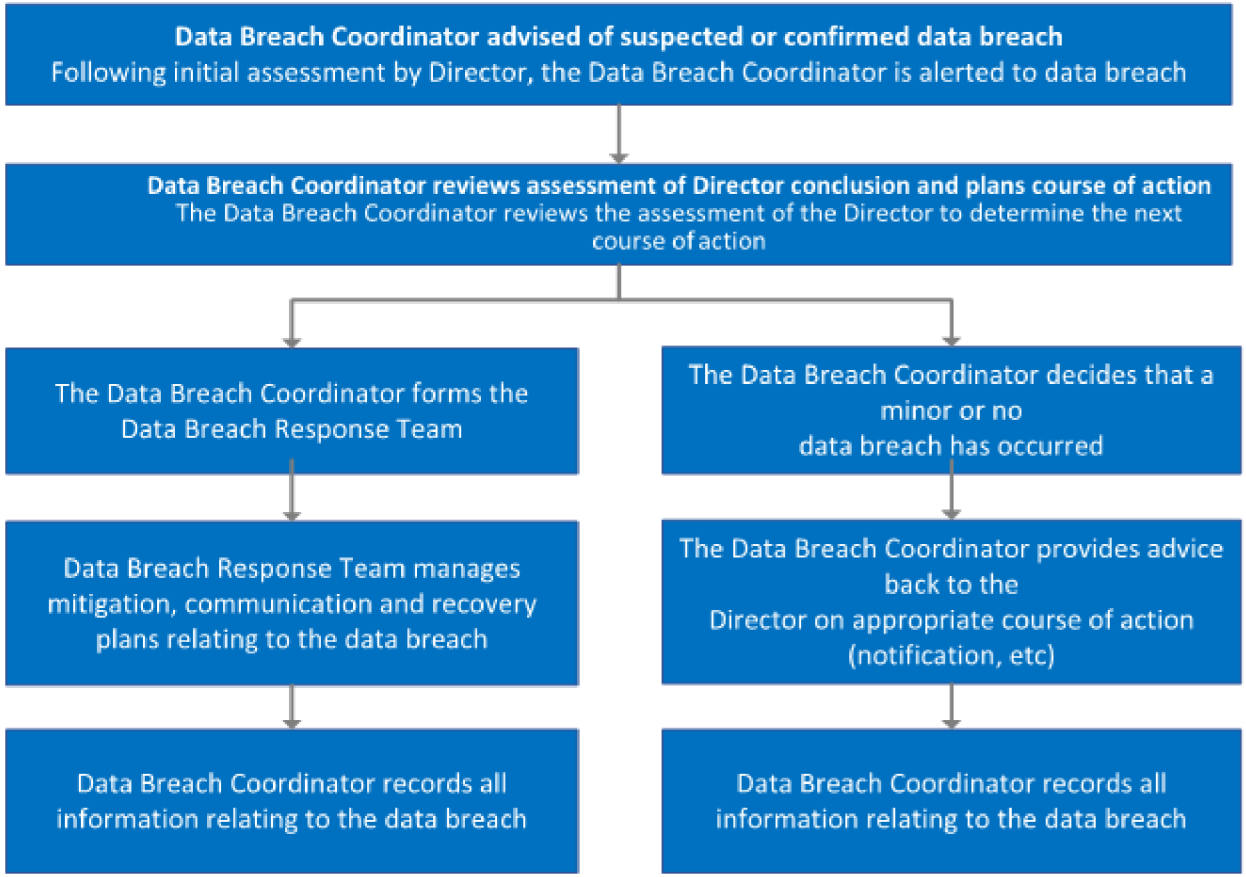
REVISION RECORD		
Approval Date	**Version**	**Revision description**
26/02/2018	1.0	Procedure approved by SEG pending additional suggestions from HR
1/04/2022	2.0	Reviewed and updated

Appendix 1 - DCP Data Breach Notification Process Overview



** The Privacy Act 1988 requires that notifications to individuals affected and the notification to the Office of the Australian Information Commissioner (OAIC) both contain specific information. See www.oaic.gov.au for more information.

Appendix 2 - Data Breach Coordinator (DBC) process



Appendix 3 – DCP Data Breach Response Checklist

The following checklist is intended to guide the response team in the event of a data breach. The Data Breach Coordinator will oversee the actions listed below and assign tasks subject to availability of staff.

Step 1: Contain the breach and make an assessment

- ☐ ICT and Information Management: to immediately contain the breach:
  - ☐ if data breach is electronic, immediately investigate ICT system security and access controls. If it is inappropriate to shut down a system, restrict access to breached system(s).
  - ☐ if breach is based on paper records, review and verify physical security.
- ☐ Assess the severity and nature of the breach.
- ☐ Ensure the assessment of the breach is completed within 30 calendar days from date of discovery, subject to the Note in Section 4.1.
- ☐ If the data breach is determined to be a minor breach, notification to individuals may not be required.
- ☐ Ensure evidence is preserved that may be valuable in determining the cause of the breach, or in undertaking appropriate corrective action.
- ☐ Document the assessment.
- ☐ Consider developing a communications or media strategy to manage public expectations and media interest.

Step 2: Evaluate the risk to individuals impacted by the breach

- ☐ Conduct initial investigation, and collect information about the breach, including:
  - ☐ The date, time, duration, and location of the breach.
  - ☐ Is the data notifiable under the Act?
  - ☐ The type of personal information involved in the breach.
  - ☐ How the breach was discovered and by whom.
  - ☐ The cause and extent of the breach.
  - ☐ A list of the affected individuals, or possible affected individuals.
  - ☐ The risk of serious harm to the affected individuals.
  - ☐ The risk of other harms.
- ☐ Determine whether the context 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: Notification of breach to individuals

- ☐ Determine who needs to be made aware of the breach (internally, and potentially externally).
- ☐ Determine whether to notify affected individuals – is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals.
- ☐ If the data is notifiable you must contact the owner of the personal information as soon as practicable[4].

- ☐ Consider whether others should be notified, including the Significant Incident Reporting Unit, police/law enforcement, or other agencies or organisations affected by the breach, or where DCP is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

[4] Practicable is defined as the most immediate and appropriate time since the data breach was discovered.

Step 4: Lessons learned to prevent future data breaches

- ☐ Fully investigate the cause of the breach.
- ☐ Report to the DCP Senior Executive Group and the Privacy Committee of South Australia any outcomes and recommendations:
  - ☐ Update security and response plan if necessary.
  - ☐ Make appropriate changes to policies and procedures if necessary.
  - ☐ Revise staff training practices if necessary.
  - ☐ Consider the option of an audit to ensure necessary outcomes are effected.