Notifiable Data Breach (Customer Information) Procedure

1. PURPOSE and SCOPE

1.1. The purpose of this procedure is to provide a process to report and manage suspected thefts involving data, data breaches or exposures (including unauthorised access, use, or disclosure) and to outline the response to a confirmed theft, data breach or exposure, based on the type of data involved.

1.2. UnitingSA will comply with the new Notifiable Data Breaches (NDB) government requirements and ensure that procedures are communicated to employees to minimise the occurrence of a breach and should a NDB occur, the breach is identified and dealt with as required by the Privacy Act's NDB scheme.

1.3. UnitingSA will use a data breach response plan so that employees understand their roles and responsibilities should a notifiable breach occur.

1.4. This procedure applies to all employees, contractors, volunteers and students working with UnitingSA.

2. BACKGROUND

2.1. UnitingSA complies with the Privacy Act 1988 and the Australian Privacy Principles aimed to protect personal information which belongs to individuals by placing restrictions on how that information can be collected, handled, used and disclosed.

2.2. Commencing on 22 February 2018, changes to the federal Privacy Act make it compulsory for organisations to notify specific types of data breaches e.g. NDBs, to individuals affected by the breach and to the Office of the Australian Information Commissioner (OAIC).

2.3. The NDB amendment to the Act was introduced due to recommendations from the Australian Law Reform Commission which found that as more and more information was being held in electronic format, the risk of breaches in security protecting that data was also greatly increased.

2.4. UnitingSA collects personal Information from customers/clients, potential customers, employees, volunteers, website visitors, business contacts, donors and a range of other stakeholders.

2.5. Some kinds of personal information breaches are more likely than others to cause serious harm e.g. those that involve sensitive information such as medical or health information, information or documents commonly used for identity theft (e.g. Medicare details, driver's license or passport information) or financial information. Combinations of different types of personal information (as opposed to a single piece of information) may be more likely to result in serious harm.

Notifiable Data Breach (Customer Information) Procedure

3. DEFINITIONS

3.1. A data breach occurs where "personal information held by an organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse." E.g. a computer is stolen from an office or from an unlocked vehicle, a cloud storage app is hacked, employee back up records are lost, a computer virus allows unauthorised access to customer data or personal medical or sensitive data is sent to another customer by mistake, hard drive and other storage media being disposed without the contents first being erased, unauthorised publishing of classified information to an uncontrolled environment e.g. the internet or social media.

3.2. Not all data breaches will be NDBs. A NDB is defined as a data breach that is likely to result in **serious harm** to any of the individuals to whom the information relates.

3.3. Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to UnitingSA's reputation or brand or one of our stakeholder's reputation or brand.

3.4. Under the Act a data breach must be notified where:

3.4.1. There is unauthorised access to, or unauthorised disclosure of, personal information; and

3.4.2. Personal information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and

3.4.3. Assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in **serious harm** to any of the individuals to whom the information relates. Examples of a data breach which may meet the definition of an eligible data breach include when:

- A device containing customer personal information is lost or stolen e.g. a laptop;
- A database containing personal information is hacked; or
- Personal information is mistakenly provided to the wrong person.

4. PROCEDURE

4.1. UnitingSA will ensure that personal information is managed in an open and transparent way. This requires us to:

4.1.1. Implement practices, procedures and systems to ensure compliance with privacy laws and appropriately handle any enquires or complaints about privacy;

4.1.2. Have a clear and up to date Privacy Policy that documents the way we manage personal information effectively.

4.1.3. Report an NDB to the Office of the Australian Information Commissioner (OAIC) and any affected individuals.

4.2. UnitingSA will have robust systems in place so that data is protected and a breach does not arise, as well as comply with Australian Privacy Principle 11, which requires an organisation to take 'reasonable steps' to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

5. WHERE AN ELIGIBLE DATA BREACH HAS OCCURRED

5.1. Any employee who suspects that a theft, breach or exposure of UnitingSA protected data or sensitive data has occurred must immediately advise and provide a description of what occurred to their Manager. The Manager will then notify their Executive Manager. The Response Team to be convened by the Executive Manager Strategy and Service Improvement will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred.

5.2. If the incident is a suspected theft then SAPOL will also be contacted. The name of the SAPOL service and the report number should be provided to the Executive Manager Strategy and Service Improvement.

5.3. There is no single method of responding to a data breach. Data breaches must be dealt with 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.

5.4. Where an eligible data breach is suspected or believed to have occurred, UnitingSA must:

5.4.1. Immediately contain the breach and do a preliminary assessment and investigation. Collect information about the breach promptly, including:

- The date, time, duration, and location of the breach;
- 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.

5.4.2. Convene a response team to handle the breach or exposure. The Executive Manager Strategy and Service Improvement will coordinate this process. The team will include members from:

- Information Services: if a theft, breach or exposure has occurred, the Information Services team will follow the appropriate internal IS procedures depending on the class of data involved;
- Marketing and Communications: A communications or media strategy to manage public expectations and media interest may be required. Materials that may need to be developed to handle the incident may include: web pages, a notification letter, a press release (s), Q&A for media and Q&A for call centre and other responders;
- The Privacy Officer;
- A representative from the Risk Committee;
- The affected service or department that uses the involved system or output or whose data may have been breached or exposed;
- Additional departments based on the data type involved e.g. Finance Services regarding financial details, including but not limited to credit card numbers, bank account numbers, investment details etc.
- Additional individuals as deemed necessary.

- Carry out a risk assessment and assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This must be as prompt and efficient as practicable in the circumstances; and
- Taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

5.4.3. Prepare a statement of prescribed information regarding an eligible data breach that is believed to have occurred. The statement must set out:

- The identity and contact details of UnitingSA;
- A description of the eligible data breach that UnitingSA has reasonable grounds to believe has happened;
- The kind/s of information concerned; and
- Recommendations about the steps that affected individuals should take in response to the eligible data breach that the organisation has reasonable grounds to believe has happened.

5.4.4. Submit the statement to the Office of the Australian Information Commissioner; and

5.4.5. Contact all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums. A range of options are available to manage this including:

- Option 1 – Notify all Individuals

  If it is practicable, UnitingSA can notify each of the individuals to whom the relevant information relates e.g. all individuals whose personal information was part of the data breach.

  This option may be appropriate, and the simplest method, if we cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people.

  The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified and allowing them to consider whether they need to take any action in response to the data breach.

- Option 2 – Notify only those Individuals at Risk of Serious Harm

  If it is practicable, UnitingSA can notify only those individuals who are at risk of serious harm from the eligible data breach.

  If UnitingSA identifies that only a particular individual, or a specific group of individuals, involved in an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified.

- Option 3 – Publish Notification

  If neither option 1 or 2 above are practicable, UnitingSA must:

  Publish a copy of the statement on our website and take reasonable steps to publicise the contents of the statement.

  It is not enough to simply upload a copy of the statement prepared for the Commissioner on any webpage of the UnitingSA's website. We must also take proactive steps to publicise the substance of the data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

5.4.6. Prevent future breaches by evaluating what occurred and implementing risk management strategies to prevent a future occurrence of the incident.

6. HANDLING COMPLAINTS

6.1. If an individual wishes to make a complaint about privacy data breaches, that person is to contact the Privacy Officer who will investigate the complaint by using the steps described in the UnitingSA External Complaints Resolution Policy.

6.2. Customers can lodge a complaint with us about any breach of our Privacy Policy and our privacy obligations by contacting the Privacy Officer.

Privacy Officer Enquiries: 70 Dale St. Port Adelaide SA 5015

Notifiable Data Breach (Customer Information) Procedure

PH: (08) 8440 2200

7. RECORDKEEPING

7.1. Personal and sensitive information is managed using the UnitingSA Records Management disposal schedule.

7.2. All records relating to customer information must be retained in accordance with the UnitingSA Records Management Procedure.

8. DOCUMENTATION

8.1. Notifiable Data Breach Notification Letter

9. REFERENCES

9.1. Privacy Policy

9.2. Code of Conduct Policy

9.3. Risk Management Policy

9.4. Records Management Procedure

9.5. External Complaints Resolution Policy

9.6. Information Security Management Policy

9.7. Network Information Management Procedure

9.8. Information Sharing Procedure

9.9. Aged Care Accessing Written Information Guidelines

9.10. Customer Information Management Procedure (Community Services)

9.11. Penelope Case Noting Procedure