P276	DATA BREACH RESPONSE PROCEDURE

Policy context: This policy relates to	
Legislation or other requirements	Privacy Act 1988 Australian Privacy Principals
Contractual obligations	

POLICY STATEMENT

Enhanced Lifestyles (EL) and Lifestyle Assistance and Accommodation Service (LAAS) are committed to protecting the privacy and personal information that it holds about individuals. Enhanced Lifestyles and Lifestyle Assistance and Accommodation Service will act appropriately and in a timely manner in the event of a data breach, to contain the possible resulting harm and notify individuals affected as required.

The document complies with NDIS Practice Standards 2018, standard 1.3 Privacy and Dignity, 2.2 Risk Management, 2.4 Information Management and ACIS 2018, section 1.3 Service Users Dignity and Privacy, 2.2 Risk Management, 2.4 Information Management, 2.6 Reporting.

This document is readily available to all Customers/Clients and employees of Enhanced Lifestyles and Lifestyle Assistance and Accommodation Service including The Boards.

Definitions

Data Breach: When personal information held by an organisation is disclosed accidentally, lost, or accessed without permission. This can be as a result of human error, or through malicious action by an employee or an external party.

Examples include where a secure IT system containing personal information has been hacked, a storage device being lost by an employee, or an employee accidentally releasing personal information to the wrong person.

Personal information: 'Information about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.'[1]

Personal information includes a person's health information, tax file number, and information about racial or ethnic origin, sexual orientation or criminal record.

[1] *Privacy Act 1988,* Section 6

P276	DATA BREACH RESPONSE PROCEDURE

Data breach response team

The response team is responsible for assessing, investigating, notifying and reviewing data breaches. Roles and responsibilities are to be established and communicated prior to a data breach occurring.

Team leader: Chief Executive Officer or Chief Operations Officer

Responsibilities:

- Leading the response team and assigning tasks
- Reporting incident to governing body
- Reporting incident to Government bodies

Information Technology: IT Officer

Responsibilities:

- Liaising with IT providers
- Collecting information to report
- Ensuring implementation of any corrective action plan

Human Resources: GM Corporate Services

Responsibilities:

- Liaising with any employees affected by the data breach
- Providing assistance to employees affected

Communications: GM Quality, Learning & Development/GM Business Development & Culture

Responsibilities:

- Creating communication about the breach and it's affects
- Bringing Customer/Client questions to the Team Leader
- Answering questions from Customers/Clients

Procedure

Identify

When staff have reason to believe there has been a data breach, they should inform the COO and/or the CEO immediately.

At this time, details such as when and how the breach was discovered, and by whom, should be recorded.

Contain

As soon as a breach or suspected breach has been identified, any steps to contain or limit the potential harm should be taken. This may include shutting down a system that has been breached, or recovering any records.

The staff member who discovers the breach will complete a preliminary assessment of the breach and take any immediate action to contain the breach if possible. If actions such as the shut down of certain systems or applications is required to contain the breach then these actions will require the approval of the COO or CEO to go ahead. The COO or CEO will then facilitate an on the spot action plan to facilitate continued services while the breach is being dealt with.

Assess

If the preliminary assessment finds that further investigation and assessment is necessary to understand the nature and extent of the breach, it will be escalated to the data breach response team. The team will work together to gather information, assess risks and the likelihood of serious harm from the breach, and therefore whether it is an 'eligible' (notifiable) breach.

To evaluate whether a known data breach is notifiable, consider the following three questions:

- **Has there been unauthorised access, unauthorised disclosure, accidental loss, or theft of personal information that the organisation holds?**
  For example, the organisation's database is hacked, a portable storage device containing personal information is lost, or the organisation accidentally releases personal information to the wrong person.

- **Is it *likely* that this may result in <u>serious</u> harm to individual/s whose data has been breached?**

  This can include but is not limited to psychological, financial, emotional, physical or reputational harm. To be able to accurately assess the likelihood and seriousness of harm, it requires looking at the context of the data and how it may have been breached.

For information about the factors to consider when deciding whether harm is likely and/or serious, refer to section 26WG of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*

- **Does the likelihood of serious harm remain despite taking available remedial action?**
  The obligation to notify the OAIC can be avoided if the organisation takes remedial action in a timely manner to prevent the risk of harm occurring, either by making the harm unlikely to occur, or non-serious.

If the answer to the above three questions is yes, then the breach classifies as an eligible data breach and organisations are required to notify the OAIC and any affected individuals.

If there are reasonable grounds to *suspect* that there has been a data breach, the data breach response team should conduct an assessment of the suspected breach. The assessment of a suspected breach must take place within 30 days of it occurring, and should seek to find out the likelihood of serious harm occurring as a result of the suspected breach. If it is assessed to be likely, this has the same notification obligations as a known data breach under the NDB Scheme.

The Data Breach Response team will work together to investigate, respond and formalise an action plan in response to any data breach.

Take remedial action

Remedial action can be taken at any point throughout the data breach response process – the sooner the better. However, it may be that the full extent and nature of the breach, and therefore the actions that could be taken, are not known until after assessing and investigating the breach.

Examples of remedial action include remotely deleting sensitive information from a laptop which has been lost, or emailing affected individuals with advice to change their password details for an online account for which login information may have been hacked.

The data breach response team should document the process of any remedial action, making sure to document rationale and reasoning as to why a certain conclusion has been made.

If, after the remedial action has been taken, the risk of harm is reduced so that it is unlikely to occur, or non-serious, then there is no requirement to notify.

Even if there is no requirement, however, the data response team should consider whether to contact affected individuals with advice for further protecting their information as a customer service measure.

Notify

Once a breach has been assessed as eligible, relevant individuals and bodies should be notified as soon as practicable. Notification must include the following information as a minimum:

- The organisation's name and contact details
- Description of the data breach
- Type of information involved in the breach
- Advice and recommendations for individuals to take in response

1. **The OAIC**

The CEO is responsible for notifying and liaising with the OAIC for data breaches which have been assessed as eligible for the purposes of the Notifiable Data Breaches Scheme, using the OAIC's Notifiable Data Breach form.

2. **Notification of individuals who are at likely risk of serious harm due to the data breach**

The way notification occurs will depend on the context and nature of the breach, and the relationship of the individuals affected to the organisation. It should occur as soon as practicable after completing the notification statement for the OAIC.

In circumstances were a data breach affects only a couple of individuals these individuals will be contacted in a personal and direct manner, either face to face, verbally over the phone or by mail. If a person with disability is affected by the data breach, then the offer of having an independent advocate be present to support them will be made.

If the data breach affects a significant number of people or is particularly serious in nature, then a notification of the breach will be distributed to all Customers/Clients. This could be done using the monthly newsletter or as a separate publication, whichever would be most timely.

Notification to affected individuals may contain an explanation of what happened to their personal information, an apology, description of what measures have been put in place as a result of the breach, and advice on what they can do to further protect their information.

Record and review

Data breach log

A data breach log will record all instances of data breaches or suspected breaches, as well as document assessments of the breach and any changes made as a result of a breach.

All staff should be made aware of the log, and the Quality team will be responsible for ensuring that all breaches or suspected breaches are recorded accurately in the log.

Review

Whether or not the breach or suspected breach was notifiable, a review should be conducted into processes relating to the breach to strengthen protections in the future. Depending on the type and seriousness of the breach, this may include:

- A full investigation into how the breach occurred
- Implement measures to ensure it does not reoccur, documented in a prevention plan
- Reviews of security, cybersecurity and ICT policies and procedures
- Audit of implementation of relevant policies and procedures
- Additional staff training about privacy and data breach responses

DOCUMENTATION

Documents related to this policy	
Related policies	Data Breach Policy
Forms, record keeping or other organisational documents	