Q276	DATA BREACH POLICY

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) understand the importance of the personal and sensitive information we have been entrusted with by our Customers/Clients, employees and other stakeholders and our responsibility to report any breaches that affect the privacy of this information.

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 Customer/Clients and employees of Enhanced Lifestyles and Lifestyle Assistance and Accommodation Service including The Boards.

Introduction

The Privacy Act 1988 (Cth) and the Australian Privacy Principles protect personal information which belongs to individuals by placing restrictions on how that information can be collected, handled, used and disclosed.

Personal information must be managed in an open and transparent way. This requires us to:

- Implement practices, procedures and systems to ensure compliance with privacy laws and appropriately handle any enquires or complaints about privacy;
- Have a clear and up to date Privacy Policy that documents the way we manage personal information, including:
    - The kinds of information we collect;
    - How we collect and hold it;
    - The purposes for which we collect, hold, use, disclose it;
    - How people can access and correct the information we hold about them;

- How people can make a privacy related complaint and how we deal with such complaints; and
- Whether we are likely to disclose information to overseas recipients and if so, where they will be located;

- Report any 'eligible data breach' to the Office of the Australian Information Commissioner (OAIC) and any affected individuals.

Our Q108 – Privacy Policy outlines the way in which we collect hold, use and disclose personal information.

The Data Breach Response Procedure outlines how we manage any potential privacy breaches.

What is Personal Information?

Personal Information is information or an opinion about an identified individual or an individual who is reasonably identifiable. It does not matter whether it is true or whether it is oral or in writing.

In effect, it is information or an opinion that can identify a person, for example, their name, physical description, address, date of birth, sex, phone number, email address, driver's license number and information about their employer/place of work, salary and employment, business activities, investments, assets and liabilities – or any combination of these.

Sensitive personal information is information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, trade or professional association or trade union, religious or philosophical beliefs or affiliations, sexual preferences, criminal record or health information (including biometric and genetic information).

What is a Privacy Breach?

A privacy breach when we hold personal information about an individual and breach:

- Our legal obligations in relation to its collection, handling, use or disclosure; or
- The provisions of our Q108 – Privacy Policy.

When you identify an actual or possible breach, report it to Management immediately.

What is an Eligible Data Breach?

When an 'eligible data breach' occurs, we must usually report it to the OAIC and affected

individuals within strict timeframes. However, this may not be required if we act quickly to manage the breach and ensure that it will not cause any serious harm to an individual.

A privacy breach is an eligible data breach if it results in:

- Unauthorised access to or disclosure of personal information; or
- Information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur,

and this is reasonably likely to result in serious harm to an individual.

What is serious harm?

Serious harm can include identify theft and serious physical, psychological, emotional, financial or reputational harm.

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, drivers 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.

Who should report a breach?

If an eligible data breach involves personal information that you and another organisation hold (e.g. an outsourced service provider or joint venture partner), only one party needs to assess and report the breach to the OAIC and affected individuals If no-one undertakes the assessment or makes the report you could both be liable for a breach of the requirements.

As a general rule, the entity that has the most direct relationship with the affected individual(s) should report the breach.

Q276	DATA BREACH POLICY

DOCUMENTATION

Documents related to this policy	
Related policies	Q108 – Privacy Policy Q109 – Customer Records Policy Q272 – Information Management P276 – Data Breach Response Procedure
Forms, record keeping or other organisational documents	