AIMS Privacy Management Plan

AIMS collects personal information from time to time relating to clients or members, or in the performance of its RTO operations.

Purpose

The purpose of this policy is to protect the privacy of individuals and organisations about whom AIMS collects and/or holds information.

This policy outlines the guidelines which must be observed when collecting, storing and using personal and confidential information.

Compliance with Privacy Requirements

AIMS deals with personal information In accordance with the Privacy Act 1988 and the standards for NVR registered RTOs. Both standards will apply to members, employees, students and all contracted personnel

Information related to personal details of any employee, member, contractor or student is protected under the Privacy Act 1988. The 13 Privacy Principles (APPs) from the Privacy Act 1988 (Cth) form the basis of AIMS privacy policy. The APP's are principles or rules about collecting, using and disclosing personal information.

The APP's also cover keeping information secure, paying attention to data quality and accuracy, being open about collection and information handling practices, providing anonymity where possible and protection when transferring personal information to others.

The way we handle and store information on members, students and employees and contractors is a major compliance requirement for our Institute. To that end we will make every endeavour to ensure that the principle for security is incorporated into our data collection and storage procedures.

This principle is concerned with security and is about looking after the personal information we collect.

The main obligation of this principle is to keep personal information safe when it is in use and to dispose of it securely when you are finished with it. AIMS will:

- Have secure computer passwords and lockable filing cabinets;
- Check an individual's identity when they ask for access to the personal information we hold about them;
- Keep personal information away from those who do not need to see it – employees and contractors as well as members
- Destroy information securely;
- Raise security awareness with all personnel; and
- Review procedures from time to time.

Students as well as members, contractors and employees may access their personal records and files and any other Information held by AIMS by making a request in writing to the Executive Officer.

Responsibilities for Managing Privacy

Responsibilities for the management of personal information are the domain of any individual within the Institute with access to, or responsibilities for, such information.

To ensure best practice in regard to privacy AIMS promotes specific responsibilities to certain individuals / positions.

Those individuals will then be in a position to ensure that all employees and contractors are suitably instructed either through training or the introduction of policies and procedures, as to their obligations in relation to the protection of personal information in their handling.

Web Manager

Web managers need to recognise that consideration of privacy issues will affect web content in a number of ways:

- Personal information of employees and contractors presented to the public or other employees and contractors;
- Personal information of members of the public included in web documents;
- Obtaining personal information from the public through their visit to the website.

The Executive Officer is responsible to ensure that the Web Manager – whether an AIMS employee or contracted organisation is aware of their responsibilities for privacy and works within the standards for dealing with personal information that may be contained on the AIMS website.

A Privacy Statement for website use is also published on the AIMS web site.

Managerial Responsibilities

It is the responsibility of the Executive Officer, in their capacity as manager of the Institute, to prepare the organisation's Privacy Management Plan, and put in place procedures to ensure that these principles are observed in the collection, use, storage, or disclosure of personal information.

Personal information also applies to information relating to employees and contractors of the Institute

The Executive Officer is responsible for:

- Ensuring training practices are in place for employee and contractor training in privacy requirements;
- Protecting employee, contractors, students and member privacy