Privacy and Data Management Plan

Table of Contents

Purpose and Scope

This Privacy and Data Management Plan sets out how [Company Name] manages personal information and other sensitive data to protect the privacy, safety and rights of workers, clients, customers, and other stakeholders. It is designed to integrate with existing Work Health and Safety (WHS) systems so that privacy and data security risks are managed alongside other workplace hazards.

This plan applies to all workers, including employees, contractors, labour hire workers, volunteers, students and visitors who access or handle information or data on behalf of [Company Name]. It covers all business units and worksites, including:

- Office and corporate environments (e.g. administration, HR, finance, IT)
- Retail and wholesale operations (e.g. point-of-sale systems, loyalty programs, online stores, inventory systems)
- Disability and aged care services (e.g. client records, care plans, incident reports, medication charts)
- Security services (e.g. CCTV footage, access control logs, incident reports, patrol records)

The plan applies to information in any form, including paper records, electronic files, emails, databases, cloud systems, CCTV footage, photographs, audio recordings and portable media.

Objectives

The objectives of this Privacy and Data Management Plan are to:

- Protect the confidentiality, integrity and availability of personal information and other sensitive data
- Support compliance with WHS legislation, privacy laws, and other relevant standards and codes of practice.
- Identify and control WHS risks associated with data handling, including psychological harm, reputational damage, and operational disruption.
- Provide clear guidance to workers on their responsibilities for handling information securely and lawfully.
- Ensure that data is collected, used, stored, shared and disposed of in a way that is necessary, proportionate and respectful.
- Provide clear processes for responding to privacy incidents, data breaches and WHS-related information security events.

Definitions

Key Terms

- **Personal information**: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not, and whether recorded in material form or not.

- **Sensitive information**: A subset of personal information that includes health information, disability information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, and criminal record.
- **Health information**: Information or an opinion about the physical, mental or psychological health or disability of an individual, including health services provided or to be provided.
- **Worker**: Any person who carries out work in any capacity for [Company Name], including employees, contractors, subcontractors, labour hire workers, apprentices, trainees, volunteers and work experience students.
- **WHS**: Work Health and Safety, including obligations under relevant Australian WHS legislation and regulations.
- **Data breach**: Unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information that [Company Name] holds.
- **Information asset**: Any data, record or information system that has value to [Company Name], including paper files, electronic records, databases, applications and CCTV systems.

Legislative and Regulatory Context

[Company Name] will manage privacy and data in accordance with applicable legislation, standards and codes, including (as relevant to jurisdiction and industry):

- WHS Acts and Regulations for the relevant Australian state or territory
- Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs)
- NDIS Act and NDIS Practice Standards (for disability services)
- Aged Care Act and Aged Care Quality Standards (for aged care providers)
- Fair Work Act 2009 (Cth) – in relation to employee records
- Surveillance Devices Acts and workplace surveillance laws (for CCTV and monitoring)
- Health records legislation and codes where applicable
- Industry-specific codes of practice and professional standards

This plan should be read in conjunction with [Company Name]'s:

- WHS Policy
- Risk Management Procedure
- Incident Reporting and Investigation Procedure
- Records Management Policy
- Information Security Policy
- Code of Conduct

Roles and Responsibilities

Officers and Senior Management

Officers and senior managers must exercise due diligence to ensure that [Company Name] complies with WHS and privacy obligations. This includes:

- Ensuring adequate resources and systems are in place to manage privacy and data risks.
- Approving this Privacy and Data Management Plan and monitoring its implementation.
- Ensuring privacy and data risks are included in WHS risk registers and reviewed regularly.
- Reviewing incident and breach reports and ensuring corrective actions are completed.

Managers and Supervisors

Managers and supervisors are responsible for implementing this plan in their areas of control. This includes:

- Ensuring workers receive training on privacy, data handling and WHS implications.
- Identifying and controlling data-related risks in their work areas (e.g. retail point-of-sale, care documentation, security monitoring rooms, corporate offices).
- Ensuring access to information systems is limited to those who need it for their role.
- Ensuring secure storage, transmission and disposal of records.
- Responding promptly to privacy concerns and escalating potential breaches.

Workers

All workers must:

- Follow this plan and any related policies and procedures.
- Only collect, access, use or disclose information that is required for their role.
- Keep passwords and access credentials secure.
- Report any suspected data breaches, lost devices, misdirected emails or other privacy incidents.
- Maintain confidentiality of client, customer, worker and organisational information.
- Participate in training and refreshers as required.