

IT3 - IT PRIVACY &
MONITORING
POLICY

Purpose

Freightways respects the privacy of its users and seeks to foster a climate free from arbitrary or capricious monitoring of employees and the records they create, use or control. However, because Freightways provides some latitude for IT users to conduct Freightways business off-site and to conduct personal matters at their place of work, Freightways data and private data may be in the same place. IT users should consider issues of privacy when storing their own data on Freightways IT resources.

Freightways must at times access data and monitor **IT resources**. This policy identifies the special circumstances in which an authorised **IT user** may access another person's private data that is held on **IT resources**.

Policy Application

This policy applies to all members of **Freightways group** whether at a **Freightways site** or elsewhere and refers to all IT resources.

Definitions

Term	Definition
Authorised	Refers to an IT user who has been given permission to access the requested data by a member of the Freightways executive team or their delegates within Unit .
Private data	All data that is not Freightways data and is generated and/ or stored by an individual for their own use.
IT resources	Refers to any Freightways owned or operated hardware or software and the data that is used or stored on it.
IT user	Means any individual member of the Freightways group using IT resources.
Heads of unit	General Managers, Freightways CEO, Freightways CFO, Freightways CIO
Unit(s)	Refers to an organisational grouping across Freightways and includes Business Units, Internal Service providers.
Freightways	Freightways Limited and its subsidiary companies together or individually as the context implies.
Freightways Group	includes all staff members (whether permanent, temporary or part time), contractors, subcontractors, consultants, business partners or official visitors or guests of members of Freightways staff.

Key Relevant Documents

Include the following:

- Privacy Act 2020 (NZ)
- Privacy Act 1988 (AU)
- Freightways - IT Security Policy
- Freightways - IT Acceptable Use Policy
- Freightways - Offensive Materials Policy

Roles and Responsibilities

Freightways group staff must maintain awareness and adherence to applicable IT policies, standards and guidelines.

Heads of unit are responsible for communicating and applying IT policies, standards and guidelines within their unit.

Policy

1. **Authorised IT users** may access or monitor the content of **private data** where lawfully and reasonably required to do so by **Freightways**, including in the following circumstances:
 - 1.1. Where **Freightways** has the permission of the **IT user**.
 - 1.2. Where **Freightways** is required by law to disclose data held on **IT resources**.
 - 1.3. When **Freightways** has reasonable grounds to suspect that the law or any **Freightways** policy may have been breached.
 - 1.4. To avert reasonably anticipated significant threats or hazards to **IT resources**.
 - 1.5. When it is necessary for **Freightways** to determine whether data under the control of an **IT user** are **Freightways** data, and the IT user is either unavailable or unwilling to give consent to access such data.

Other IT-related policies

This IT Privacy and Monitoring Policy should be read in conjunction with all other Freightways IT-related policies.