

20 July 2026

Scott Rowbottom

Email: fyi-request-34942-76c17855@requests.fyi.org.nz

Our ref: OIA 133803

Tēnā koe Scott.

Official Information Act request: Information management and privacy controls

Thank you for your email of 23 June 2026 to the Ministry of Justice (the Ministry). Under the Official Information Act 1982 (the Act), you requested:

1. *Details of the measures in place to comply with section 3.4 of the Information and Records Management Standard.*
2. *Details of the measures in place to comply with Information Privacy Principle 5 (IPP5).*

In response to your request;

1. Measures in place to support section 3.4 of the Information and Records Management Standard

The Ministry supports compliance with section 3.4 of the Information and Records Management Standard through a combination of governance, operational, privacy and information security controls. These include policies and guidance governing information security, information management, access management, record handling, retention and disposal, and the protection of information from unauthorised access, alteration, loss, deletion or destruction. The Ministry also maintains security monitoring, audit capabilities, access management controls and security incident management processes. These measures support the protection of information and records wherever they are located and assist in ensuring access controls are implemented and maintained.

Within the Public Defence Service (PDS), additional operational measures include:

- mandatory induction and ongoing training for lawyers and support staff covering privacy, confidentiality, legal privilege, security awareness, risk management and information handling;
- compliance requirements under the Ministry's Code of Conduct, the PDS Code of Conduct, relevant ICT policies, and PDS policies relating to confidentiality, disclosure and conflicts of interest;
- documented processes governing the handling and disclosure of client information;
- use of the Affinity practice management system for client and matter information, with staff receiving training in its use and being required to access information only for legitimate work purposes;

- physical safeguards including secure handling of client correspondence and disclosure material, protection of information in work areas, and secure disposal of documents; and
- privacy and security incident reporting processes, including the use of the Ministry's Haumarū system.

2. Measures in place to support Information Privacy Principle 5

Information Privacy Principle 5 requires agencies to take reasonable safeguards to protect personal information against loss, unauthorised access, use, modification, disclosure and other misuse.

The Ministry supports compliance with IPP5 through governance, operational and security measures. Relevant controls are set out in Ministry policies and guidance governing the secure handling, storage, access, sharing, retention and disposal of personal information. Supporting guidance requires staff to protect personal information through measures such as secure storage practices, appropriate handling of physical and electronic records, protection of passwords and access credentials, secure transfer methods, and safeguarding information from inappropriate access or disclosure.

The Ministry also undertakes privacy assurance activities, including privacy assessments to identify and manage privacy risks associated with new or changed initiatives. Security monitoring, audit capabilities, access management controls, and privacy and security incident management processes support the ongoing protection of personal information.

Within the Public Defence Service, further measures include:

- mandatory privacy, confidentiality, legal privilege and security awareness training for lawyers and support staff;
- professional and organisational obligations requiring staff to protect confidential and legally privileged information;
- restrictions on the disclosure of client information, including processes governing who may access and share information;
- privacy breach reporting and management processes, including the use of the Ministry's Haumarū system;
- document handling and physical security practices designed to reduce the risk of unauthorised access, disclosure, loss or misuse of information; and
- compliance with the Ministry's Code of Conduct, the PDS Code of Conduct and related policies governing the use and protection of personal information.

Further information regarding the Ministry's privacy obligations and privacy framework is available on the Ministry of Justice website. Information about the Public Defence Service and its services is available at [Public Defence Service | Public Defence Service](#)

Please note that this response, with your personal details removed, may be published on the Ministry website at: [Official Information Act responses | New Zealand Ministry of Justice](#).

If you are not satisfied with this response, you have the right to make a complaint to the Ombudsman under section 28 of the Act. The Office of the Ombudsman may be contacted by phone on: 0800 802 602, by email at: info@ombudsman.parliament.nz, or via the webform: [Make a complaint \(for members of the public\) | Ombudsman New Zealand](#).

Yours sincerely

Peter Hutchinson

Peter Hutchinson
Director, Public Defence Service