

21 August 2026

Dear [REDACTED]

Thank you for your request made under the Official Information Act 1982 (OIA), received on 3 August 2026. You requested the following:

- 1. A list of all systems operated by your agency that fall within the scope of the [Biometrics Processing Privacy Code 2025](#) as of 3 August 2026*
- 2. Copies of proportionality assessments as required under Rule 1(1)(d) of the [Biometrics Processing Privacy Code 2025](#), or a Privacy Impact Assessment that meets that requirement, for each system in the list*

Systems Subject to the Biometrics Processing Privacy Code 2025

Inland Revenue operates two systems that fall within scope of the Biometrics Processing Privacy Code 2025:

- **Windows Hello for Business** – used as an option for staff to log into a work device.
- **Voice ID** – optional verification service for customers.

Proportionality Assessments

I am releasing the proportionality assessments completed for Windows Hello for Business and Inland Revenue's Voice ID system to you in full, attached as an **Appendix**.

Publishing of OIA response

We intend to publish our response to your request on Inland Revenue's website (ird.govt.nz) as this information may be of interest to other members of the public. This letter, with your personal details removed, may be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the OIA's purpose of enabling more effective participation in the making and administration of laws and policies and promoting the accountability of officials.

Thank you again for your request.

Yours sincerely

[REDACTED]
Dawn Swan
Privacy Officer - Integrity

Appendix - Proportionality Assessments

Windows Hello for Business

Windows Hello for Business (WHfB) as an authentication method for Inland Revenue staff accessing their assigned IR-managed device. WHfB is optional and replaces password-based sign-in with device-based authentication using either a PIN or biometric method, such as facial recognition or fingerprint recognition.

The user's biometric information is converted into a mathematical template and stored locally on the user's device. Biometric data is not stored centrally by Inland Revenue, does not roam with the user, and is not sent to Microsoft or an external user.

WHfB is used to strengthen authentication for staff accessing IR systems and devices and reduces risks such as credential theft and phishing. This supports IR's function of protecting systems and taxpayer information. The lawful purpose of the processing is to secure the device and verify the user.

Inland Revenue has considered the scope, extent, and degree of privacy risk associated with WHfB biometric processing and has assessed that the use of biometric information is proportionate to the likely impacts on individuals.

Biometric use is proportionate and necessary because:

- it is voluntary; IR staff are not required to use it and alternative log-in methods remain available;
- it provides stronger authentication than passwords;
- biometric information is saved on the device and secure; and
- it is limited to authentication purposes only
- there is no impact on the privacy of individuals.

Voice ID

Voice ID is a voice-biometric tool that analyses the distinctive characteristics of a person's voice to create a biometric template, commonly referred to as a voiceprint, for identity verification. When a customer enrolled in Voice ID calls IR, their voice is compared to the saved biometric template.

IR collects biometric information solely for Voice ID purposes. The biometric information is used for security validation, customer authentication, and access management of customers within IR contact centre services.

Voice ID is an opt-in service. Customers choose whether to enrol and must first be validated by an IR staff member before enrolment can occur. Voice ID is available to customers aged between 16 and 99 years and can only be enrolled against an individual's own account. Voice ID cannot be established or used on behalf of another customer, including a nominated person or representative. Where a customer has chosen to enrol, Voice ID is used to verify their identity against their individual account.

IR considers the collection and processing of biometric information for Voice ID to be lawful and proportionate for the purpose of securely authenticating customers and protecting customer information from unauthorised access. Biometric processing is used because it provides an effective means of verifying a customer's identity and supports the prevention of identity fraud and account compromise. Alternative authentication methods remain available for customers who choose not to enrol; however, Voice ID provides enhanced security and authentication capabilities that cannot be achieved as effectively in all circumstances through non-biometric methods alone.

In accordance with the Biometric Processing Privacy Code 2025, IR has considered the scope, extent, and degree of privacy risk associated with Voice ID processing and has assessed that the use of biometric information is proportionate to the likely impacts on individuals. This assessment takes into account the security and fraud-prevention benefits of Voice ID, the voluntary nature of enrolment, the availability of alternative authentication methods, and the safeguards applied to the collection, use, storage, and protection of biometric information.

IR considers that the public and individual benefits of improved identity assurance, enhanced protection of personal information, reduced risk of unauthorised access, and a more secure customer authentication process outweigh the residual privacy risks associated with Voice ID processing.

Engagement undertaken as part of the assessment identified that biometric information, including voiceprints and voice recordings, have particular cultural significance for Māori.

A Māori voice is not solely a technical identifier. It may be connected to an individual's reo, mita, whānau, hapū, iwi, whakapapa, mana, and mauri.

As a result, biometric voice information may be regarded as a taonga (treasured possession) and its collection, use, storage, retention, disclosure, and disposal have the potential to engage Māori cultural values and expectations.

The assessment identified several tikanga-based concepts that may be relevant to the processing of biometric information:

- Rangatiratanga (authority and self-determination): the importance of individuals exercising meaningful authority over their biometric information, including informed authorisation for collection, voluntary participation, and ongoing control over the use and deletion of their information.
- Kaitiakitanga (guardianship): Inland Revenue's responsibility to act as a trusted custodian of biometric information and to implement safeguards governing the collection, use, storage, protection, retention, and disposal of that information.
- Whakapapa (relationships and connection): recognition that voice and language may have a direct connection to identity, culture, ancestry, and relationships, and may therefore be viewed as more than a technical authentication factor.
- Manaakitanga (care and respect): the expectation that biometric information is managed respectfully, transparently, and with an appropriate duty of care throughout its lifecycle.

A key theme identified through engagement was the importance of transparency, informed choice, and customer control. Voice ID is an opt-in service, and customers choose whether to enrol. Feedback highlighted the importance of ensuring individuals understand the sole purpose for which biometric information is collected, where it is stored, how it is protected, who may access it, how long it is retained, and the options available to withdraw from the service and request deletion of their biometric information.

Feedback also emphasised the importance of free, prior, and informed consent. Where customers provide biometric information for the purpose of Voice ID authentication, there is an expectation that the information will only be used for that purpose and will not be shared, reused, integrated into other datasets, or used for unrelated activities without appropriate authorisation. Concerns were also raised regarding the potential future use of biometric information, including the creation of profiles, datasets, or other uses enabled by emerging technologies such as artificial intelligence.

Appropriate safeguards are in place, including validation and verification processes, access controls, security protections, and governance measures intended to ensure biometric information is collected, used, retained, and protected appropriately. These controls support Inland Revenue's role as custodian of biometric information and align with the principle of kaitiakitanga.