

6 August 2026

s9(2)(a)

Tēnā koe s9(2)(a)

Thank you for your email, received on 3 August 2026, to Oranga Tamariki—Ministry for Children (Oranga Tamariki) requesting information on biometric systems. Your request has been considered under the Official Information Act 1982 (the Act).

You have requested:

- *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*
- *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*

Two systems in Oranga Tamariki fall within the scope of the Biometrics Processing Privacy Code 2025 as of 3 August 2026.

Both are biometric verification, both opt-in, and both storing the biometric template encrypted on the device only. They are:

- Windows Hello facial recognition on Ministry-issued laptops
- Face ID unlock on Ministry-issued iPhones

In May 2026, Oranga Tamariki completed an assessment of both systems against all thirteen rules of the Code, including the proportionality requirement under rule 1(1)(d), in April 2026. The assessment concluded that the collection and use of biometric information for device verification is compliant with the Code, raises no significant privacy risks, and is likely to represent a net cybersecurity and privacy benefit because it reduces reliance on passwords and PINs, which can be shared, lost or inadvertently disclosed.

A copy of this assessment is attached as Appendix One. Please note that the names of non-senior staff have been redacted under section 9(2)(g)(ii), to maintain the effective conduct of public affairs through the protection of Ministers, members of organisations, officers, and employees from improper pressure or harassment.

IN-CONFIDENCE

Other systems in the Ministry do not contain biometric-related capabilities or do not have them turned on.

Oranga Tamariki may make the information contained in this letter available to the public by publishing this on our website with your personal details removed.

I trust you find this information useful. If you wish to discuss this response with us, please feel free to contact OIA_Requests@ot.govt.nz. Alternatively, you are advised of your right to also raise any concerns with the Office of the Ombudsman. Information about this is available at www.ombudsman.parliament.nz or by contacting them on 0800 802 602.

Nāku noa, nā

A handwritten signature in blue ink, consisting of a large loop followed by a smaller loop and a short horizontal stroke.

Arun Rajamani
Chief Technology Officer
People Culture and Enabling Services

Memo

To: Marcin Betkier

CC: [REDACTED]

From: [REDACTED]

Date: 4/5/26

Security level: Low

**This memo may contain legal advice and be legally privileged.
It should not be disclosed on an information request, without further legal advice.**

Biometrics – New Regulations

Purpose

This memo provides an assessment under the Biometrics Code of the current collection and use of biometric information by Oranga Tamariki.

Background

The Privacy Commissioner has issued a Biometric Processing Privacy Code 2025 (the “Code”) that creates specific privacy rules for agencies (businesses and organisations) using biometric technologies to collect and process biometric information. [060825-Biometric-Processing-Privacy-Code-2025-A1102662.pdf](#) The Code contains 13 rules which are modifications of corresponding Information Privacy Principles from the Privacy Act 2020

Biometric information is information about a biometric characteristic like facial features, fingerprints, keystroke patterns, voice, or the way someone walks, that is used for the purpose of biometric processing by a computer- or technological-based system.

Biometric processing means the comparison or analysis of the biometric information by technology to either verify, identify or categorise a person.

Currently, Oranga Tamariki, only collects and uses biometric information for user verification¹ through facial recognition technology and fingerprint identification. The devices that incorporate this technology are:

- (1) Laptops, through ‘Windows Hello’ face recognition (Windows Hello); and

¹ Biometric verification involves the automated verification of an individual, by comparing their biometric information with their previously collected biometric information. For example, a mobile phone fingerprint scanner compares an individual's thumbprint with a stored version of the same thumbprint. Biometric verification is a one-to-one process.

- (2) iPhones, through facial recognition screen unlock and fingerprint authenticator apps (iPhone screen unlock).

As these use cases are for verification, they constitute biometric processing and therefore require an assessment of the rules under the Code.

Rules	Windows Hello / iPhone screen unlock	Assessment
Rule 1(a) Is the Collection for a lawful purpose?	Purpose for collection is for secure user authentication to access their own device and services	Satisfactory.
Rule 1(b) Is this collection necessary to effectively meet this purpose & are there no alternatives which can meet this purpose as effectively?	'Hello Windows' and iPhone screen unlock are effective for verification. While there are several alternatives which could meet this purpose such as PIN/password, they cannot do so as effectively or without additional privacy risk.	Satisfactory
Rule 1(d) Is the biometric processing proportionate to the likely impacts on people, including cultural impacts on Māori?	Risks including cultural impact of these use cases is likely to be low: use is individual, both with opt-in consent, device-based and not population-level.	Satisfactory
Rule 2 Is the source of the biometric sample from the individual concerned?	Biometric data is collected directly from the device user.	Satisfactory
Rule 3 Has Oranga Tamariki taken reasonable steps to make people aware of the collection and why it is being collected?	Collection is opt-in and users are made aware of this option during the device set up.	Satisfactory
Rule 4 Is the means of collection lawful, fair, and not unreasonably intrusive?	As facial recognition and fingerprint ID is being used solely for the purpose of device verification, and is opt-in at the user's discretion, it is unlikely to be considered unreasonably intrusive.	Satisfactory
Rule 5 Is the information collected protected from unauthorised disclosure by sufficient safeguards and stored securely?	Collected information is encrypted and stored in the local device. It is not centrally shared with the Ministry.	Satisfactory

Rule 6 Can an individual request access to their biometric information?	Not applicable as Oranga Tamariki does not hold biometric information other than what is kept in the device itself.	Not applicable
Rule 7 Can an individual request that their biometric information be corrected?	Facial and fingerprint profiles can be deleted and re-entered at the user's discretion.	Satisfactory
Rule 8 Is the information held accurate and up to date?	As the information is entered directly into the device by the user, it is expected to be accurate and up to date in the device.	Satisfactory
Rule 9 How long will the information be retained?	Facial and fingerprint profiles are retained in the devices until the user chooses to delete them. Facial and fingerprint profiles are otherwise deleted when the devices are returned and reset	Satisfactory.
Rule 10 What are the limits on the use of the biometric information?	All biometric information collected is used solely for verification and not categorisation.	Satisfactory
Rule 11 Will the biometric information be disclosed to another agency or person?	Biometric information held in the devices cannot be shared with another agency or person.	Satisfactory
Rule 12 Will the biometric information be disclosed outside of New Zealand?	No.	Satisfactory
Rule 13 Will there be unique identifiers attached to the biometric information?	No.	Satisfactory

Privacy risks and benefits

Collection of biometric information for verification ensures accurate verification of kaimahi with minimum impact on the individual. Use of facial recognition and fingerprint ID reduces the privacy risk associated with passwords and PIN numbers which can be shared, lost, or otherwise inadvertently disclosed.

However, kaimahi have noted that facial recognition technology is sensitive and the user can unintentionally unlock a device with a glance. This particular privacy risk should be managed through guidance and comms to raise awareness.

Additionally, the iPhone may be unlocked by holding it up to the kaimahi's face. This risk may also be somewhat managed through personal safety guidance and awareness.

Overall, use of this technology appears to be a net benefit with respect to privacy as sharing of passwords or PINs is a more common and difficult to manage occurrence.

Conclusion

The biometric information that Oranga Tamariki collects and uses for device verification is compliant with the Code, raises no significant privacy risks, and may indeed be a net privacy benefit.

In both use cases, the biometric information is:

- o Collected directly from the kaimahi;
- o Stored locally on their device;
- o Used only for verification purposes; and
- o Fully optional, with non-biometric alternatives available, e.g., password/PIN