RESIST KIT

GUIDE

PASSPORTS & BIOMETRIC PRIVACY

IMPORTANT DISTINCTION

Applying for an Australian passport requires providing biometric information (your photograph and, if requested, fingerprints).

This is not part of the Digital ID system at present.

Passport biometrics are collected under the Australian Passports Act 2005 and managed according to the Department of Foreign Affairs and Trade (DFAT) Privacy Policy.

This page explains what you must provide, what is optional, and how to minimise unnecessary biometric or data exposure.
If privacy feels overwhelming, you don't have to do *everything*.

1. Why Biometrics Are Required for Passports

Under the Passports Act 2005, the Australian Government requires a biometric facial image to:

- confirm identity
- prevent fraud and duplicate passports
- comply with international border standards

These requirements apply to everyone who wants a passport. They are **not voluntary,** and they are not part of the Digital ID Act 2024 - **therefore, you cannot insist that an alternative method of verification be required.**

2. What Biometrics Are Collected for Your Australian Passport

Mandatory:
A compliant passport photograph (a biometric facial template is generated from this image)

Possible (but rare) additional biometrics:
Fingerprints, but only in limited circumstances such as fraud investigations or identity concerns.

What is not collected at present:

- DNA
- Voice prints
- Iris scans
- Behavioural biometrics

3. How Passport Biometrics Are Used

Biometric data is used for:

- Verifying your identity in DFAT systems
- International border checks
- Preventing duplicate or fraudulent passport applications

By law, DFAT must handle biometric data in accordance with the Australian Privacy Principles and DFAT's own Privacy Policy.

4. How to Reduce Biometric and Data-Privacy Risk

While you *must* provide a passport photo, you can reduce unnecessary data exposure by following these steps.

A. Limit Additional Information Provided
When applying:

- Only provide information required by the form.
- Avoid volunteering extra details or documents unless requested.
- Double-check that optional fields are left blank.

B. Use a Secure Application Channel

- Apply physically in person at an Australia Post outlet rather than uploading digital photos online.
- Avoid using public Wi-Fi when submitting any online forms.
- Use a separate email address used only for government interactions (helps reduce cross-linking of data).

C. Provide Hard-Copy Photos, Not Digital Files
Whenever possible, bring physical passport photographs rather than sending digital images. Hard-copy photos reduce your digital footprint and limit metadata leakage (e.g., location data, device identifiers).

PASSPORTS & BIOMETRIC PRIVACY Continued

GUIDE

D. Do Not Consent to Additional Uses
DFAT sometimes requests permission for additional identity checks or data matching. Say no unless it is legally required.

E. Keep Your Passport Application Number Private
This number links directly to your identity and should not be shared outside the application process.

F. Request Information on How Your Data Is Stored

You may ask DFAT:

- Where your biometric template is stored
- Who it is shared with (e.g., border agencies)
- How long it is retained
- How to request access or correction of your personal information

See email template under point 5 below.

5. Email Template: Request for Information

About My Passport Biometrics
Subject: Request for Information About Biometric Data Handling - Passport Application

Dear DFAT Privacy Officer,

I am writing to request information about how my biometric data is collected, stored, used, and shared under the Australian Passports Act 2005. I make this request under the Privacy Act 1988 (Cth), the Australian Privacy Principles.

Could you please provide:

1. The specific biometric data retained in relation to my passport application.
2. Where this biometric data is stored and for how long.
3. The agencies or third parties my biometric data may be shared with, including any international data exchanges.
4. The security protections applied to that data.
5. How I may request access to, or correction of, the information held about me.

Thank you for your assistance.
Kind regards,
Name Name
DOB
Application number, if applicable

6. Key Points to Remember

- Passport biometrics are mandatory and not part of the Digital ID system.
- DFAT is legally responsible for handling biometric data under its Privacy Policy and the Passports Act.
- You can minimise additional data exposure by limiting optional disclosures and choosing safer submission methods.
- You have the right to ask how your biometric data is used, stored, and shared.

7. For more tips on reducing your digital footprint when travelling

See our Travel Privacy Guide: How to Reduce Digital & Biometric Exposure When You Travel.

ALIGNED COUNCIL OF AUSTRALIA
RCR .media