Australian Government
Department of Health

Privacy policy for COVIDSafe app

Find out how we manage any personal information we collect about you when using the app.

The Australian Department of Health, with the support of the Digital Transformation Agency in its role as the COVIDSafe IT service provider, (**we, us, our**) is implementing COVIDSafe to help States and Territory health officials (**health officials**) conduct contact tracing to stop the spread of COVID-19.

Contact tracing is a fundamental element of a public health response to disease outbreak. It is the process of identifying people who may have come into contact with someone who has COVID-19, so that they can be advised to take measures to help stop the further spread of COVID-19 (such as getting tested or self-isolating).

This privacy policy sets out how personal information that is collected via COVIDSafe will be handled in accordance with the *Privacy Act 1988* and the Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements — Public Health Contact Information) Determination 2020 (Biosecurity Determination).

What personal information will be collected, and why is it being collected?

We collect personal information to help conduct contact tracing when you register for, use or upload, data to COVIDSafe.

When you register for COVIDSafe

We will ask you to consent to the collection of your:

- **mobile phone number** — so that you can be contacted if needed for contact tracing
- **name** — so the relevant health officials can confirm they are speaking to the right person when performing contact tracing. This will be easiest if you provide your full name, but you can use a pseudonym or fake name if you prefer
- **age range** — so health officials can prioritise cases for contact tracing, if needed
- **postcode** — to make sure health officials from the right State or Territory who work in your area can contact you, and to prioritise cases for contact tracing, e.g. hotspot areas

If you are under 16 years of age, your parent or guardian will need to consent to the collection of your registration information and contact data.

When you use COVIDSafe

Your app will only record the following **contact data**: (1) the encrypted user ID, (2) date and time of contact and (3) Bluetooth signal strength of other COVIDSafe users with which you come into contact. This information will also be recorded on the other users’ devices.

An encrypted user ID will be created every 2 hours. This will be logged in the National COVIDSafe data store (**data store**), operated by the Digital Transformation Agency, in case you need to be identified for contact tracing.

No location data (data that could be used to track your movements) will be collected at any time. No user will be able to see the contact data stored on their device as it will be encrypted. Any attempt to decrypt contact data is an offence. Contact data stored on a device will be automatically deleted after 21 days.

We cannot access any contact data stored on a device, or share this with health officials, unless and until a COVIDSafe user consents to upload the data to the data store.

If you test positive to COVID-19

A health official will contact you and ask for consent to enter your mobile number into the data store to generate a PIN to be sent to you by SMS.

If you enter the PIN, you will give your consent to upload contact data on your device into the data store to share with health officials to enable contact tracing.

If another user tests positive to COVID-19, they may upload their contact data, which may include details of their contact with you.

How will personal information be collected?

Use of COVIDSafe is completely voluntary. You can install or delete COVIDSafe at any time.

As part of your use of COVIDSafe, we will collect:

- your registration information after you successfully enter a PIN sent by SMS
- information about your encrypted user ID when you have COVIDSafe open or running on your device
- information that you have tested positive to COVID-19 when you agree to a health official sending you an SMS to enable you to upload your contact data
- your contact data, when you or another COVIDSafe user you have come into contact with tests positive to COVID-19 and chooses to upload contact data on their device

No user should feel pressured to install or continue to use COVIDSafe, or to agree to upload contact data to the data store. This is prohibited under the Biosecurity Determination. If you feel pressured to do any of these things, you can make a complaint to us (see below), the Office of the Australian Information Commissioner, or the Australian Human Rights Commission.

How will personal information be stored?

We will store all registration information, encrypted user IDs and contact data, in the data store. It is a cloud-based facility, using infrastructure located in Australia, which has been classified as appropriate for storage of data up to the ‘protected’ security level.

We will delete all data in the data store after the COVID-19 pandemic has concluded as required by the Biosecurity Determination.

Contact data on your device will be automatically deleted from your device 21 days after contact occurs. It will also be deleted if you remove COVIDSafe from your device or upload your contact data to the data store.

How will personal information be used and disclosed?

We will use or disclose your personal information to enable contact tracing by health officials. This includes:

- using your mobile number to send you an SMS to confirm your number or upload your contact data
- using encrypted user IDs in uploaded contact data to identify other COVIDSafe users that a positive COVIDSafe user had contact with in the last 21 days (**contact users**)
- providing health officials with access to the registration information and contact data of contact users to enable contact tracing

Contact users may be advised to take such measures as are required by their State or Territory (such as self-isolating). Failure to comply with these measures may be in breach of State or Territory law.

We will also use or disclose your personal information to:

- ensure the proper and lawful functioning of COVIDSafe
- if it is necessary, prosecute a breach of the law in relation to contact tracing under the Biosecurity Determination and the Biosecurity Act 2015

We will not use or disclose your personal information for any other purpose.

Data about generation of encrypted user IDs to create de-identified reports about uptake of COVIDSafe will be prepared by the Digital Transformation Agency. We will also receive de-identified analytical data from iTunes and Google Play about COVIDSafe including the number of downloads, average use time and deletions.

Can personal information be deleted?

We will delete any of your personal information held in the data store when you make a request via Health web request form.

You can also uninstall COVIDSafe at any time. This will automatically delete all information stored on your device and stop other users from collecting your contact data.

Uninstalling COVIDSafe will not automatically delete any information already uploaded to the data store, or any of your contact data stored on another user's device in the last 21 days, which could still be uploaded to the data store and used for contact tracing purposes. If you wish any of your contact data uploaded to the data store to be deleted you can expressly ask us to delete your information.

Can a user correct or access personal information?

You can:

- change your registration information by deleting and re-installing COVIDSafe
- delete the registration information we hold in the data store by contacting us
- register the correct information on COVIDSafe

To ensure maximum security of your COVIDSafe data, you will not be able to access your data held in the data store.

Further information about privacy

As well as this policy, we have an Australian Department of Health privacy policy.

You can obtain a copy of the privacy policy by contacting us using the contact details set out at the end of this notice. The privacy policy contains information about:

- how you may complain about a breach of:
    - the Australian Privacy Principles (APP)
    - a registered APP code that binds us, and
    - how we will deal with such a complaint.

Contact us

Departmental privacy enquiries

Contact to find out more about privacy within the Department, or to make a privacy enquiry or complaint.

Privacy officer: privacy@health.gov.au

Phone: 02 6289 1555

Freecall: 1800 020 103

Postal address:

MDP 62, GPO Box 9848, Canberra ACT 2601