

Chief Commissioner's Instruction

The following instruction is issued pursuant to the powers of the Chief Commissioner of Police under section 60, Victoria Police Act 2013. This Chief Commissioner's Instruction was originally published on the Victoria Police intranet on 22 November 21 and is effective from that date. This instruction expires 12 months from publication or until earlier cancelled or reissued.

CCI 05/21 COVIDSafe data

Context

COVIDSafe is an application (app) that securely records when a person has been in close contact with other users of the app, in order to facilitate contact tracing. Users of the COVIDSafe app cannot access the contact data stored on their device as it is encrypted, and health officials can only access the information with the consent of the COVIDSafe user.

To assist in preventing and controlling the spread of COVID-19 the *Privacy Amendment (Public Health Contact Information) Act 2020* (Cwth) was introduced. This Act amended the *Privacy Act 1988* (Cwth) (the Act) to provide privacy protections for COVIDSafe data, and users, in order to encourage public acceptance and uptake of COVIDSafe and enable faster and more effective contact tracing.

The purpose of this CCI is to provide instructions to employees in relation to the access, use and storage of COVIDSafe data.

This CCI was initially issued on 29 July 2020 as CCI 01/20. This CCI reissues and replaces CCI 01/20 which expired on 29 July 2021.

Scope and application

This policy applies to all employees.

References

This CCI is supported by and should be read in conjunction with the following:

- *Privacy Amendment (Public Health Contact Information) Act 2020* (Cwth)
- *Privacy Act 1988* (Cwth)

Definitions

The following definition applies to this CCI:

- COVIDSafe – an application made on behalf of the Commonwealth, for the purpose of facilitating contact tracing in relation to COVID-19.

Also refer to the general [VPM Dictionary](#) for definitions and acronyms.

Responsibilities and procedures

Overview

1. It is an offence to collect, use or disclose COVIDSafe data, unless for a permitted purpose (s.94D the Act).
2. A limited exception to this offence exists where COVIDSafe data is incidentally collected at the same time as other data, provided that:
 - it is deleted as soon as practicable after the person becomes aware that it has been collected; and

- it is not otherwise accessed, used or disclosed by the person after it has been collected.
3. Where COVIDSafe data is incidentally collected, it cannot be used as evidence in any investigation or prosecution.
 4. Admissibility of non-COVIDSafe data as evidence in any proceedings is not affected by the incidental collection or subsequent deletion of COVIDSafe data.

Responsibilities

5. All employees must ensure that use of digital evidence collection tools, including but not limited to Cellebrite UFED, Cellebrite Touch or MSAB units does not result in the known extraction and retention of COVIDSafe app data.
6. If COVIDSafe app data is incidentally extracted, employees must:
 - redact the COVIDSafe data as soon as practicable; and
 - delete any unsanitised copies of the data
7. If the COVIDSafe data is not able to be omitted or redacted from an extraction the entire extraction must be deleted as soon as practicable.
8. If for any reason an employee receives COVIDSafe data in error, that employee must, as soon as practicable:
 - notify the custodian of that data (Informant or Cybercrime Squad); and
 - delete the data.
9. COVIDSafe data incidentally collected by Special Projects Unit (SPU), Intelligence and Covert Support Command must be deleted in accordance with local instructions.

Further advice and information

For further advice and assistance with this instruction, contact the Cybercrime Squad.