Foster Care Association of Victoria Inc.

PRIVACY POLICY

2026

fcav
foster care
association
of victoria

Authorisation

This was endorsed by the FCAV Board of Directors in May 2026.

Review date

This Policy shall be further reviewed every 12 months, or if legislative changes require an update to the Policy, or a privacy breach occurs.

Contents

1. Purpose

The FCAV regularly handles information about members, carers, children and young people in care, workers, stakeholders, donors, job applicants, and members of the public in the course of providing its services.

The FCAV is legally obliged to handle personal information in accordance with the Privacy Act. This Policy adopts the Australian Privacy Principles (**APPs**) set out in the *Privacy Act 1988* (Cth) (**Privacy Act**).

The purpose of the Policy is to provide a framework for the FCAV in managing the privacy considerations of personal information it holds. This Policy adopts the meaning of 'personal information' as defined by the Privacy Act.[1]

This Policy is publicly available on the FCAV website.

[1]Section 6(1) of the Privacy Act defines personal information as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not'.

2. Scope

This Policy applies to all FCAV Board of Directors, employees and volunteers including students on placement.

The FCAV Chief Executive Officer (**CEO**) is responsible for the implementation of this Policy, and for monitoring changes in privacy legislation. The FCAV Board of Directors is responsible for reviewing and endorsing the Policy.

3. Privacy complaints

Individuals may submit a privacy complaint to the FCAV if they believe the FCAV has mishandled their personal information or breached the Privacy Act or the APPs.

Refer to the FCAV's Feedback and Complaints Policy on our website: https://www.fcav.org.au/about-us/publications-and-policies.

4. How the FCAV handles your personal information

4.1 Collection

a. The FCAV will only collect information that is necessary for the performance and primary function of the organisation,[2] or a directly-related purpose.[3]
b. The FCAV will collect personal information only by lawful and fair means.[4]
c. It will notify stakeholders about why the information is collected, how it is administered, and how the information may be accessed by the individual.
d. Where possible, the personal information will be collected from the individual themselves,[5] unless it is unreasonable or impracticable for the FCAV to do so.[6]
e. Sensitive information will only be collected with the individual's consent,[7] if required by law,[8] or if permitted under the Privacy Act.[9] The Policy adopts the meaning of 'sensitive information' as defined by the Privacy Act, to include information about health, religious or philosophical beliefs, and sexual orientation or practices.
f. Sensitive information collected for statistical or reporting purposes will be anonymised or de-identified.
g. If the FCAV receives unsolicited personal information that it did not request, it must be destroyed,[10] and the person whose personal information has been destroyed will be notified about the receipt and destruction of their personal information.

2 APP 3.2
3 APP 3.1
4 APP 3.5
5 APP 3.6
6 APP 3.6
7 APP 3.3(a)
8 APP 3.4(a)
9 APP 3.4(b) lists out 'permitted general situations' where the FCAV is permitted to collect sensitive information, for example to lessen or prevent a serious threat to the life, health or safety of any individual.
10 APP 4.14

4.2 Use and disclosure

a. The FCAV will only use or disclose information for the primary purpose for which it was collected or a directly related purposes.[11] If personal information is used for other purposes, the FCAV will seek the individual's consent. [12]

b. If information is used for direct marketing purposes, such as to promote the services of FCAV to its members,[13] the FCAV will take the following steps:

- collect only a minimal amount of information, such as an email or mailing address;
- provide an accessible form of opting out; and
- ensure marketing communications include the FCAV's business address, email address and phone number.

c. The FCAV may also disclose personal information if required by law, or to assist in regulatory or legal investigations.

d. The FCAV will not sell, rent or trade personal information it holds.

e. The FCAV will also not input personal information into Artificial Intelligence (**AI**) tools.

4.3 Social Media

a. The FCAV holds various social media accounts to engage with its stakeholders. It will not publish materials that identify children or young people in care on these platforms.

b. Where material identifying children or young people in care is posted publicly to our social media accounts, for example, by members of the FCAV, the FCAV reserves the right to remove any such material.

4.4 Openness, access and correction

a. The FCAV will take reasonable steps to ensure the personal information it collects is accurate, up-to-date, and complete.[14]

b. If an individual believes that the information the FCAV holds about them is out of date, inaccurate, incomplete, or misleading, they may write to the FCAV requesting it to correct this information. The FCAV will take reasonable steps to do so.[15]

c. If the FCAV is unable to correct the personal information, it will provide the individual with written reasons.

d. The FCAV reserves the right to withhold access of an individual to his or her information if:

- providing access would pose a serious and imminent threat to the life or health of any individual;
- providing access would have an unreasonable impact upon the privacy of individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the organisation and the individual;

11 APP 6.1
12 APP 6.1(a)
13 APP 7.2
14 APP 10.1
15 APP 10.2 and APP 13.

- providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- providing access would be unlawful; and
- providing access would be likely to prejudice an investigation of possible unlawful activity.

e. On request, the FCAV will also take reasonable steps to inform an individual about the type of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.[16]

4.5 Storage (onshore and offshore)

a. The FCAV stores personal information using both onshore and offshore service providers, including cloud-based platforms. Regardless of location, the FCAV takes reasonable steps to ensure that all providers maintain strong privacy and security standards consistent with the Privacy Act and APPs.

b. Before using any service provider, the FCAV adopts the following practices:
   - Conduct due diligence on the provider's privacy practices and security certifications (e.g. ISO 27001, SOC 2);
   - Include contractual safeguards regarding privacy, data handling and breach notifications;
   - Verify technical controls such as encryption, access management, backups and multi-factor authentication;
   - Monitor provider compliance through ongoing IT risk assessment reviews; and
   - Record provider details and storage locations in the IT Assets Register.

4.6 Destruction, anonymisation and de-identification of personal information

a. Personal information will be retained only as long as necessary to fulfil the purpose for which it was collected, to comply with legal or regulatory obligations or to support organisational needs.

b. It will be securely destroyed or de-identified once no longer required.[17]

c. Data from laptops, mobile devices and storage media are securely wiped before these devices are decommissioned.

d. The FCAV will request permission from an individual before publishing identifiable information related to them for written case studies.

e. When using information related to individuals for written case studies, the FCAV will apply pseudonyms, resulting in the individual being de-identified.

f. Where an individual prefers to communicate via a pseudonym, the FCAV will take reasonable steps to facilitate this process.

g. The FCAV will permit people from whom the personal information is being collected to not identify themselves or use a pseudonym unless it is impracticable to deal with them on this basis.

16 APP 12.1
17 APP 11.2

4.7 Information Security

The FCAV adopts the following practices on its organisational devices and information technology systems:

a. It applies access restrictions on relevant folders, systems, and applications
b. It uses password protection on all devices and multi-factor authentication for cloud and web-based services
c. It maintains external monitoring of firewall, anti-virus and other security infrastructure
d. It conducts annual IT risk management reviews of systems and processes
e. It implements appropriate safeguards to protect personal information from misuse, loss, unauthorised access, modification, interference, or disclosure
f. It maintains an IT Security Risk Assessment Register
g. Staff are required to complete Confidentiality Agreements during induction
h. Staff are provided regular training on privacy best practices.

5. Responding to a privacy breach

As an agency funded by the Department of Families, Fairness and Housing (**DFFH**), the FCAV is required to report any privacy incidents to the DFFH. In addition, the FCAV will also take the following steps to respond to a privacy breach:

a. Take immediate action to contain and investigate the breach, including identifying the root cause(s), risks, and parties affected;
b. If necessary, engage external assistance in responding to the breach and preventing further breaches;
c. Notify individuals affected by the breach; and
d. Implement further measures to prevent a similar breach from occurring in the future.

In certain circumstances, the FCAV will also be required to report a privacy incident to the Office of the Information Commissioner Australia (**OAIC**). These circumstances arise where:

a. The FCAV experiences unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information;
b. which is likely to result in serious harm to one or more individuals;[18]
c. The FCAV has not been able to prevent the likely risk of serious harm with any remedial action.

18 'Serious harm' is defined in the Privacy Act to include serious physical, psychological, emotional, financial, or reputational harm.