Foster Care Association of Victoria Inc.

PRIVACY POLICY

2023

fcav
foster care
association
of victoria

Contents

Authorisation

This policy was endorsed by the FCAV CEO and acknowledged by the FCAV Board of Directors in May 2023.

This policy shall be further reviewed every 3 years.

1 Introduction

The Foster Care Association of Victoria Inc (FCAV) is committed to protecting the privacy of personal information which the organisation collects, holds and administers. Personal information is information which directly or indirectly identifies a person.

1.1 Purpose

The purpose of this document is to provide a framework for the FCAV in dealing with information management and privacy considerations.

1.2 Policy

The FCAV recognises the essential right of individuals to have their information administered in ways which they would reasonably expect – protected on one hand, and made accessible to them on the other. These privacy values are reflected in and supported by our core values and also reflected in our Privacy Policy, which is compliant with the Privacy Act 1988.

The FCAV is bound by laws which impose specific obligations when it comes to handling information. The organisation has adopted the following principles contained as minimum standards in relation to handling personal information.

The FCAV will:

- Collect only information which the organisation requires for its primary functions.
- Ensure that stakeholders are informed as to why we collect the information and how we administer the information gathered.
- Use and disclose personal information only for our primary functions or a directly related purpose, or for another purpose with the person's consent.
- Store personal information securely, protecting it from unauthorised access.
- Provide stakeholders with access to their own information, and the right to seek its correction.

1.3 Responsibilities

The FCAV's CEO is responsible for the implementation of this policy, for monitoring changes in Privacy legislation. The FCAV Board is responsible for reviewing this policy.

This policy applies to all FCAV Board Members, employees & volunteers. The FCAV will endeavour to comply with this policy in handling Personal Information about members, carers, workers, stakeholders, donors, job applicants and members of the public.

---

2 Process

2.1 Collection

The FCAV will:

- Only collect information that is necessary for the performance and primary function of the organisation.
- Collect personal information only by lawful and fair means and not in an intrusive way.
- Notify stakeholders about why we collect the information and how it is administered.
- Notify stakeholders that this information is accessible to them.
- Collect personal information from the person themselves wherever possible.
- If collecting personal information from a third party, be able to advise the person whom the information concerns, from whom their personal information has been collected.
- Collect Sensitive information only with the person's consent or if required by law (Sensitive information includes information about health, religious beliefs, race, gender and others).
- Collecting sensitive information for use in the context of statistical information is anonymized or de-identified.
    - The FCAV will collect health information about an individual if the information is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual and for HR purposes. This information is kept in storage with strict access controls.
- Determine, where unsolicited information is received, it must be destroyed, and the person whose personal information has been destroyed will be notified about the receipt and destruction of their personal information.

2.2 Use and Disclosure

The FCAV will:

- Only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose.
- For other uses, the FCAV will obtain consent from the person.

- For marketing purposes, only an email or mailing address is collected so that marketing can be disseminated, and an opt-out is provided.
- Each written direct marketing communication with the individual must set out the FCAV's business address, email and phone number which the organisation can be directly contacted.
- Ensure any overseas providers of services are as compliant with privacy as the FCAV. Such disclosures will only be made if:
    - the overseas recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Australian Privacy Principles; or
    - the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.
- Provide all individuals access to their personal information except where it is a threat to life or health or it is authorised by law to refuse and, if a person is able to establish that the personal information is not accurate, then the FCAV must correct it.
- Where for a legal or other reason we are not required to provide a person with access to the information, consider whether a mutually agreed intermediary would allow sufficient access to meet the needs of both parties.
- If the FCAV has sufficient reasons to believe that an unlawful activity has been, is being or may be engaged in, and the disclosure of personal information becomes a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, the organisation may make such disclosures.
- The FCAV may disclose personal information if it is mandated by an enforcement body For the purpose of this Clause, the FCAV must make a written note of the use or disclosure.

2.3 Storage

The FCAV takes several steps to ensure the security of information about the people we support and to manage risks. These measures include:

- Place access restrictions on relevant folders and systems
- Password protection on all computers and Multi-Factor-Authentication on cloud and web-based applications
- Include Confidentiality Agreements in Staff Induction.
- Regular communication and training for staff to ensure confidentiality is upheld
- External monitoring of security infrastructure including firewall and anti-virus software.
- Bi-annual IT Risk Management reviews conducted of IT systems, and processes.

The FCAV will:

- Implement and maintain steps to ensure that personal information is protected from misuse and loss, unauthorised access, interference, unauthorized modification or disclosure.
- Ensure outsourced service providers such as cloud-based storage are privacy complaint and maintain strong access and security controls and procedures over who can access the data.
- The FCAV will have systems which provide sufficient security.
- Ensure that data the FCAV holds is up to date, accurate and complete.

2.4 Destruction and de-identification

- Destroy personal information once is not required to be kept for the purpose for which it was collected, or after seven years, in accordance with Record Keeping Standards Australia.
- Wipe data from decommissioned laptops and mobile phones.
- Change information to a pseudonym or treat it anonymously if required and not use any government related identifiers unless they are reasonably necessary for our functions.

2.5 Data Quality

- Take reasonable steps to ensure the information the organisation collects is accurate, complete, up to date, and relevant to the functions we perform.

2.6 Information Security and Retention

- Maintain an IT Security Risk Assessment Register
- Maintain Information in accordance with Record Keeping Standards Australia; https://www.ato.gov.au/business/record-keeping-for-business/overview-of-record-keeping-rules-for-business/

2.7 Openness

The FCAV will:

- Ensure stakeholders are aware of The FCAV's Privacy Policy and its purposes.
- Make this information freely available in relevant publications and on the Organisation's website.
- On request by a person, take reasonable steps to let the person know, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

2.8 Access and Correction

The FCAV will:

- Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date.
- If the individual and the FCAV disagree about whether the information is accurate, complete and up to date, and the individual asks to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation will take reasonable steps to do so.
- Withhold the access of an individual to his/her information if:
    - providing access would pose a serious and imminent threat to the life or health of any individual; or
    - providing access would have an unreasonable impact upon the privacy of other individuals; or
    - the request for access is frivolous or vexatious; or
    - the information relates to existing or anticipated legal proceedings between the organisation and the individual; or
    - 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; or
    - providing access would be unlawful; or
    - providing access would be likely to prejudice an investigation of possible unlawful activity; or

- an enforcement body performing a lawful security function asks [organisation] not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

- Provide to the individual its reasons for denial of access or a refusal to correct personal information.
- If the FCAV decides not to provide the individual with access to the information on the basis of the above mentioned reasons, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

2.9 Identifiers

- The FCAV will request permission from an individual before using information related to them for written case studies. All information used is to be de-identified, making it impossible to recognise which particular person the information is connected with.

2.10 Anonymity

- Allow 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.

2.11 Responding to a Privacy Breach

- If a suspected Privacy Breach has been reported, the FCAV will immediately take action to work out how the breach occurred and prevent the breach from happening further.
- The FCAV will Identify the risks to people's information and stop or mitigate any further risks.
- If required, the FCAV will notify people affected by the breach and the DFFH.
- Review the circumstances and put measures in place to prevent breaches in the future.