Foster Care Association of Victoria Inc.

PRIVACY POLICY

2014

fcav
foster care association of victoria

FCAV Privacy Policy adopted by the FCAV Board of Directors in June 2006 and an updated version on the 15th April 2014.

FOSTER CARE ASSOCIATION OF VICTORIA PRIVACY POLICY

Introduction

This policy is designed to comply with State and Federal privacy legislation where applicable.

Foster Care Association of Victoria Inc (FCAV) is committed to ensuring that the Personal Information it holds about individuals is handled appropriately and lawfully.

This policy sets out some basic guidelines for FCAV's dealing with Personal Information. For the purposes of this policy, "FCAV" also includes FCAV's associated entities.

"**Personal Information**" means information which identifies an individual or from which an individual's identity can be reasonably ascertained and includes Sensitive Information. Name, address and home telephone number are examples of Personal Information.

"**Sensitive Information**" is a sub-category of personal information. It includes information or an opinion about an individual's racial or ethnic origin, political opinions, philosophical or religious beliefs or affiliations, membership of a political, trade or professional association or trade union, sexual preference or practices, criminal record or health information.

"**Health Information**" means information or an opinion about an individual's physical, mental or psychological health, disability, health services and donation of body parts, including genetic information. This encompasses sick leave certificates, doctors' reports and medical checks.

"**Privacy Officer**" means a person that may be nominated by FCAV from time to time to perform that role.

"**Workers**" for the purposes of this policy includes employees, contractors including agency staff), volunteers, consultants and Board members of FCAV.

Application of the Policy

This policy applies to all workers. FCAV will endeavour to comply with this policy in handling Personal Information or Health Information about carers, workers, donors, unsuccessful job applicants and members of the public. The degree of compliance depends on FCAV's organisational requirements and legal or regulatory obligations.

Workers' Responsibilities

FCAV requires that all workers comply with this policy at all times and treat the Personal Information handled in the course of their employment with FCAV in a way that respects the private nature of that information.

Workers must refrain from gossip about personal details concerning others, must collect and handle Personal Information in accordance with this policy and take reasonable steps to protect any Personal Information in their care from misuse, loss, unauthorised access, modification and disclosure.

This can include measures such as:

1. Storing Personal Information in locked filing cabinets;
2. Having a clean desk policy;
3. Not allowing others to use any worker's computer passwords;
4. Good records management, including information stored electronically;
5. Not taking files out of the office (relates to point 1);
6. Destroying documents containing Personal Information instead of discarding in the general waste.

Board members and volunteers will have access to information stored on the network on the G drive.

This list is by no means exhaustive and the security measures taken should be those that are reasonable in the circumstances.

Collection of Personal Information

FCAV workers will only collect Personal Information that is necessary for FCAV's functions and activities, or to comply with legal or regulatory obligations. FCAV workers will collect Personal Information by lawful and fair means and not in an unreasonably intrusive way. When a worker collects any Personal Information, the worker must provide the relevant person information about:

- Why FCAV is collecting Personal Information;
- How to contact FCAV to gain access to the individual's Personal Information;
- The types of organisations (if any) to which FCAV may disclose the Personal Information (e.g. Department of Human Services);
- Any law that requires the particular information to be collected; and
- The main consequences for failure to provide that information;

In most cases, FCAV workers must obtain the individual's consent if they collect Sensitive Information. Exceptions include where:

- The collection is required or authorised by law;
- The individual is incapable of giving consent and the collection is necessary to prevent a serious health and safety threat; or
- The collection is necessary for defence of a legal claim;

Use of Personal Information

Personal Information will only be used for the stated primary purpose(s) for which it was collected and in some cases for related secondary purposes.

Where a FCAV worker needs to use Personal Information for purposes other than the stated purpose, they must obtain consent where appropriate and necessary. Exceptions to this include where:

- The use is required to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or to public health and safety;
- FCAV suspects fraud or unlawful activity;
- The use is necessary to assist a law enforcement agency in its law enforcement functions; or
- The use is required or authorised by law;

In such cases (except in cases of emergency, or where the use is required or authorised by law), the use of Personal Information must be authorised by the Chief Executive Officer or a Privacy Officer.

Other than in cases of emergency, Sensitive Information may only be used and accessed by FCAV workers where there is a clear and compelling organisational or other need to do so and when the use is authorised by the Chief Executive Officer or Privacy Officer.

Disclosure of Personal Information to Third Parties

FCAV workers may only disclose Personal Information to other entities (including related entities of FCAV) for the primary purpose(s) for which that Personal Information was collected, or in some circumstances for related other ("secondary") purposes.

Where a FCAV worker wishes to disclose Personal Information for purposes other than these purposes, they must obtain specific consent for any secondary purpose where appropriate and necessary.

As a general rule, FCAV will seek written consent prior to the disclosure of any personal information. In the operation of the Caregiver Information Support Service (CISS), FCAV will seek and casenote verbal permission from carers prior to the release of personal information e.g. in advocacy.

FCAV is not required to obtain consent where:

- The disclosure is required to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or to public health and safety;
- FCAV suspect fraud or unlawful activity;
- The disclosure is necessary to assist a law enforcement agency in its law enforcement functions; or
- The disclosure is required or authorised by law;

In such cases (except in cases of emergency, or where the disclosure is required or authorised by law), the disclosure of Personal Information must be authorised by the Chief Executive Officer or Privacy Officer.

Quality and Accuracy of Personal Information

All FCAV workers must take reasonable steps to ensure that any Personal Information they use or disclose is complete, accurate and up-to-date. If any FCAV worker becomes aware that any Personal Information FCAV holds is not accurate, they are required to update and correct the information if possible or to notify the Chief Executive Officer or Privacy Officer.

Retention and Destruction of Personal Information

FCAV will only keep Personal Information on file for as long as it is necessary to fulfil organisational needs or legal requirements. If a decision is made by FCAV to destroy or dispose of documents, this must be done in a secure manner.

Access to and Correction of Personal Information

FCAV is committed to allowing individuals to access Personal Information about them that it holds. All requests (for example, by a worker, carer, job applicant, donor, or member of the public) must be assessed by the Chief Executive Officer or the Privacy Officer

FCAV may decide that it is not appropriate for an individual to access their personal information in circumstances where:

- 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 other individuals (this may be relevant where information about other individuals is included on a file);
- The request for access is frivolous or vexatious;
- The information relates to existing or anticipated legal proceedings where the information would not otherwise be discoverable;
- Providing access would be unlawful;
- Denying access is required by law;
- Providing access would prejudice an investigation of possible unlawful activity;
- Providing access would prejudice law enforcement; or
- The Personal Information requested is an employee record.

If FCAV refuses a request for access to the Personal Information, FCAV will provide reasons why this is the case. If access is to be denied, this must be authorised by the Chief Executive Officer or Privacy Officer.

In cases where FCAV does not wish to grant direct access to an individual to the Personal Information held about the individual, then an agreed intermediary may be used to explain that information to the individual.

Individuals may request that Personal Information about them be corrected

Individuals may also request to correct Personal Information about that individual. The appropriate FCAV staff member may make minor corrections. If the staff member is unsure whether such correction is appropriate, or if any substantial correction is requested, they must refer to the Chief Executive Officer or to the Privacy Officer for guidance. If FCAV believes it is inappropriate to alter the information, FCAV will also provide reasons why this is the case and include a statement about the disputed facts on the relevant file.

Security

FCAV staff must take all reasonable steps to protect Personal Information and to safeguard Personal Information from misuse, loss and unauthorised access, modification and disclosure.

Complaints Procedure

If individuals have any concerns about the way in which their Personal Information is being handled, or they believe that there has been an interference with the privacy of Personal Information, they may contact the Chief Executive Officer or Privacy Officer.

Complaints will be handled impartially and as promptly as possible in the circumstances. Only those people who are involved in the investigation of the complaint will have access to Personal Information in relation to the complaint unless a staff member reasonably requires access in order to fulfil their duties.

Any staff member found to have breached this policy will be subject to appropriate disciplinary action. This may include dismissal.

Where a member of the public makes a complaint about their Personal Information being inappropriately handled, then that complaint should be immediately referred to the Chief Executive Officer or Privacy Officer.

Further Information

For questions or further information about privacy and the handling of personal information, please contact the Chief Executive Officer or Privacy Officer

FCAV Privacy Policy adopted by the FCAV Board of Directors in June 2006 and an updated version on 15th April 2014.