# Privacy Policy

# Section 1 - Purpose and Objectives

(1) CFA is committed to protecting the personal information and health information that we collect, hold, manage, use, disclose and transfer.

(2) This policy supports the CFA's need to collect information and the right of the individual to privacy.

(3) It ensures that the CFA can collect personal information and health information necessary for its services and functions, while recognising the right of individuals to have their information handled in ways that they would reasonably expect and in ways that protect their personal and health information.

# Section 2 - Scope

(4) This policy applies to all CFA members and any person interacting with CFA or CFA services.

# Section 3 - Policy

(5) CFA will only collect personal information to perform its services and functions and achieve its objectives.

(6) Personal information and health information collected by CFA will be held securely.

(7) Personal information and health information collected will be used only for the primary purpose for which it was collected or as otherwise permitted by law.

(8) CFA members will handle personal information and health information on a confidential basis and not disclose personal information or health information to any third party, including colleagues, unless authorised to do so.

### Personal Information

(9) Personal information (or personally identifiable information) is information about an individual, whether fact or opinion, from where their identity is clear or where someone could reasonably work out that it related to the individual. The amount and type of personal information CFA collects about a person depends upon the nature of CFA’s relationship with them and their requirements from CFA.

(10) Where CFA requests that a person provide their personal information and they elect not to provide it, CFA may not be able to provide them with some or all of its services or if they are a CFA member, it may impact their involvement with CFA.

(11) Some personal information is considered particularly sensitive and this type of information is subject to higher protections. Sensitive information includes information about an individual’s race or ethnicity, political opinions, religion, philosophical beliefs, membership to trade or association or union, sexual preferences or criminal record.

(12) CFA may also collect health information. CFA will only collect this information where necessary for one or more of its functions, such as assessing an individual’s ability to perform a role, volunteer or workers' compensation where

they have consented and in accordance with the Health Privacy Principles (the HPPs) under the Health Records Act 2001.

## Collection of Personal Information

(13) Personal information will only be collected or solicited for a lawful purpose that is directly related to a function or service of CFA, and is reasonably necessary for that purpose.

(14) Information is collected wherever possible from an individual directly. When CFA collects information from an individual we inform them why we are collecting it and how we intend to use it, through a notice called a collection notice. Our aim is to collect it lawfully, fairly and without undue intrusion. At the time the information is collected, CFA will advise in general terms of any other individuals or organisations that have access to the information and whether there are any consequences of not providing the information.

(15) If CFA needs to collect sensitive information about an individual, consent will be sought to do so unless otherwise authorised by law.

## Use and Disclosure of Personal Information

(16) CFA uses information only for the purpose for which it was collected or a logically related purpose that an individual would reasonably expect (in the case of sensitive information for a directly related purpose) unless consented to another specific use.

(17) In some circumstances, CFA is required or authorised by law to release information such as:

a. To lessen or prevent a serious threat to an individual's life, health, safety or welfare.
b. To lessen or prevent a serious threat to public health, public safety or public welfare.
c. Where CFA suspects unlawful activity has occurred and using or disclosing your personal information is necessary to investigate or report the activity.
d. Where CFA is required by law to release the information.
e. It is necessary for research that is in the public interest and will not be published in a way that identifies individuals and it is impracticable to seek the individuals consent.
f. Where the information is used to manage, evaluate or improve particular services in relation to which the information was originally collected.

(18) An individual's contact details may be used by CFA or its contracted service providers, bound by confidentiality agreements, to survey them about their experience with CFA.

(19) CFA only transfers personally identifying information outside the state of Victoria where this is required for the purpose for which it was collected or if required by law. CFA seeks to ensure the information is afforded the same level of privacy protection it would receive in Victoria.

## Data Quality

(20) Wherever possible, CFA will seek to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date. In many instances CFA relies upon an individual to provide accurate and complete information and to advise CFA if their circumstances change over time.

(21) CFA takes reasonable steps to ensure the information it holds is accurate, complete and up to date. In accordance with the Public Records Act 1973, an individual's personal information may be deleted after the requisite period of time has elapsed, or where it is no longer required for any purpose. This prevents the holding of information that may be out of date or incorrect. Retention requirements will be considered in conjunction with other relevant laws that may

effect whether CFA is permitted to delete or remove information.

## Data Security

(22) CFA seeks to protect personal information from misuse, loss, unauthorised access, modification, or disclosure. CFA securely destroys or de-identifies personal information when it is no longer needed for any purpose. Where personal information is provided to a contracted third party for the performance of a CFA service, that party is bound by contract to ensure the information is treated with the same level of privacy protection as it would be afforded by CFA.

(23) Some of CFA's third-party service providers operate outside the state of Victoria or Australia. CFA will endeavor to ensure that these providers handle personal information in accordance with Victorian privacy and data security obligations.

## Access and Correction

(24) An indvidual has the right to access and correct information their that is held by CFA. In most cases, requests for access will be administered in accordance with the Freedom of Information Act 1982, particularly requests that may affect the privacy of another individual or relate to commercial activity. Where another statute stipulates the way access to personal information should be given or an amendment made, that Act's direction will be followed.

(25) CFA members should ensure that they keep their details up to date within the approved membership database.

(26) CFA members seeking to make their contact details silent within the CFA wide directory may do so by selecting the relevant 'keep private' option within Members Online. Private contact details will remain visible to some CFA members due to CFA's operating requirements. For CFA volunteers this may include CFA employees, FRV Secondees and Brigade Management Teams.

(27) Where CFA holds health information that is later established by an individual to be inaccurate, incomplete, misleading or not up to date, we will take reasonable steps to correct the information. However, in accordance with the Health Privacy Principles, CFA may not be able to delete the inaccurate information unless otherwise stipulated in the Health Records Act 2001 or required by Law. Corrections to records will likely be made in the form of a notation or alteration of the record in accordance with the Privacy and Data Protection Act 2014.

## Unique Identifiers

(28) A unique identifier is a code consisting of alphabet characters and numerals (not a person's name) which is applied to an individual instead of their name and distinguishes them from other individuals, for example a CFA employee or member number. CFA uses unique identifiers so that it can carry out its services and functions efficiently.

(29) The use of unique identifiers between organisations are prohibited except in specific circumstances to reduce the extent of harm and identity theft.  Where CFA issues a unique identifier it does not share it with other organisations unless it is necessary for CFA to carry out any of its functions effectively, we have obtained your consent or is otherwise permitted or authorised by law.

(30) CFA assigns a unique identifier to CFA members and labour hire contractors to facilitate interactions within CFA.

## Anonymity

(31) Wherever it is practicable and lawful, CFA seeks to allow an individual to interact anonymously with CFA. However, anonymity is not considered to be practicable in relation to being a CFA member, the completion of billing for services provided by CFA, Patient Care Records or Fire/Incident Reports.

## Complaints

(32) Individuals may make a complaint to the Privacy Officer about a CFA act or practice that they believe is an interference with their privacy via privacy@cfa.vic.gov.au. The Privacy Officer will investigate the complaint.

(33) Individuals can also make a complain directly to the Office of the Victorian Information Commissioner (OVIC) and the Health Complaints Commissioner if they have complained to CFA and are concerned about or have not received a satisfactory response:

a. Office of the Victorian Information Commissioner (OVIC) https://ovic.vic.gov.au/privacy/for-the-public/privacy-complaints/
b. Health Complaints Commissioner https://hcc.vic.gov.au/make-complaint

## Responsibilities

| Role | Responsibilities |
|---|---|
| **Chief Information Officer / Data Officer** | Oversight for all information, and data records at the CFA.<br>Is responsible for:<br>1. technology-related privacy risk management;<br>2. the data retention and destruction framework;<br>3. the digital platforms and applications that create and store data; and<br>4. security of the CFA digital platforms.<br>5. third-party vendors or cloud service providers, overseeing the relationships, including contract management, and compliance with data security and privacy requirements and<br>6. managing the breach response plan in the event of a data breach. |
| **Contract Signatories** | CFA members who are authorised to execute contracts under the Financial Delegations are accountable for the decision to contract. Contract Signatories are therefore responsible for ensuring that they are satisfied that a contractual arrangement complies or can comply with relevant legislation (including privacy legislation), this Policy and that appropriate contract management arrangements are in place for the life of the Contract, before executing any contract. |
| **Data Owner** | A person with legal control of the information, and they're ultimately responsible for making sure it's handled correctly. They have administrative or operational responsibility for the relevant business domain's data and other information (e.g the General Manager People and Culture is responsible for employment information etc).<br>Data Custodians are responsible for ensuring appropriate safeguards are implemented for the protection of personal and health information for which they are responsible. This includes:<br>1. responsibility for who has access to the data<br>2. personal and health information collection control management;<br>3. personal and health information use/disclosure control management (including approving any proposed use of personal or health information by other areas of the CFA internally);<br>4. personal and health information data quality & destruction control management;<br>5. approving the content of any Privacy Impact Check or Assessments where the data/information for which they are responsible is involved in any project or program of work; and<br>6. privacy complaint management/remediation (on advice of Governance, Legal and Risk).<br>Legislated responsibilities:<br>1. Public Records Act 2003 (Vic) - (i) Sets requirements for creating, managing and disposing of public records.<br>2. Privacy and Data Protection Act 2014 (Vic) - (ii) Defines obligations for handling personal information. |
| **Data Custodian / Data Stewards (Optional Role)** | Responsible for supporting the Data Owner in the day-to-day management of information in accordance with privacy legislation.<br>Legislative Responsibilities:<br>1. Public Records Act 2003 (Vic) - (i) Assists owner in ensuring records meet requirements. Fits within overall information governance framework. |

| Role | Responsibilities |
|---|---|
| **Data Users** | The person or team/groups of people who create, receive, or get information, and they can be either CFA members within the organization or people from outside it.<br>Legislative Responsibilities:<br>1.<br>Privacy and Data Protection Act 2014 (Vic) - (i) Understands obligations for handling personal information.<br>2.<br>Public Records Act 2003 (Vic) - (ii) May have responsibilities for creating or maintaining public records. Agency policies and procedures; (iii) Adheres to specific data handling protocols. |
| **Governance Legal and Risk** | Governance, Legal and Risk is responsible for:<br>1. the ongoing review of CFA's privacy practices and providing advice to help ensure they comply with this Policy, current legislation and best practice;<br>2. advising and educating individuals of their responsibilities under privacy legislation and this Policy;<br>3. reviewing and providing advice and recommendations on privacy impact assessments and<br>4. the receipt and oversight of privacy complaints. |
| **Project Managers** | Where a project is involved, Project Managers, are responsible for ensuring a Privacy Impact Check or Privacy Impact Assessment has been completed and approved by the relevant Data Custodian(s) before personal or health information is collected or used as part of any project or program of work and that they are kept up to date throughout the life of a project. |
| **Project Sponsor** | Has overall accountability for ensuring that a project or program of work complies with or can comply with relevant legislation (including privacy legislation) and this Policy (as well as meeting its objectives, within the approved budget and delivers the projected benefits). Privacy Impact Checks and Privacy Impact Assessments are intended to assist with evidencing legislative compliance. |

# Section 4 - Definitions

(34) Commonly defined terms are located in the CFA centralised glossary.

# Section 5 - Related Documents

(35) Data and Information Governance Policy

(36) Intellectual Property Policy

(37) Security and Dash Camera Policy

(38) ICT Acceptable Use Policy

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 17th December 2024 |
| **Review Date** | 17th December 2027 |
| **Approval Authority** | Chief Executive Officer |
| **Approval Date** | 17th December 2024 |
| **Expiry Date** | Not Applicable |
| **Accountable Officer** | [redacted] General Manager Governance, Legal and Risk |
| **Responsible Officer** | [redacted] Senior Manager Governance Services |
| **Author** | [redacted] Senior Business Partner, Privacy and Compliance |
| **Enquiries Contact** | Privacy and Freedom of Information |

## Glossary Terms and Definitions

**"CFA member"** - Refers to all CFA volunteers, volunteer auxiliary workers, officers, employees and secondees.

**"CFA employee"** - Any person who is directly employed by CFA, including those employees on a fixed term or casual employment contract.

**"CFA volunteer"** - An officer, member, or volunteer auxiliary worker who receives no remuneration for their services in relation to a brigade but does not include an officer or member of an industry brigade.

**"FRV Secondee"** - An officer or employee of Fire Rescue Victoria made available to CFA under section 25B of the FRV Act.

**"Labour hire contractor"** - Personnel provided by a staffing agency for a fee. These personnel are employees of the agency and not CFA.

**"Brigade Management Team"** - The group of officers and members with the responsibility for management of the affairs and activities of the brigade and for the efficient service delivery of the brigade.

**"Personal information"** - Personal information is recorded information (or an opinion) about an individual whose identity is apparent or can be reasonably ascertained from that information, but does not include health information.

**"Health information"** - Health information is personal information which concerns an individual's physical, mental or psychological health, disability or genetic makeup or which is collected to provide, or in providing, a health service.

**"Sensitive information"** - Sensitive information is personal information about an individual's race or ethnicity, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or a trade union, sexual preferences or practices or criminal record.