

UMFC PRIVACY POLICY

POLICY INTENT

UMFC is committed to protecting and upholding the right to privacy of clients, staff, volunteers, Board Directors and representatives of organisations we deal with. UMFC is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

The purpose of this policy is to outline the following:

- reasonable/allowed collection of personal information
- storage of information
- appropriate access to information.

SCOPE

This policy applies to all clients, Board Directors and contractors of UMFC.

Personal and sensitive information handled by UMFC is managed in accordance with the privacy principles contained in the *Privacy and Data Protection Act 2014* (Vic) and the *Privacy Act 1988* (Cth) (the Privacy Act). Other requirements, like client confidentiality and legal privilege, are managed separately in accordance with specific service or practice requirements, such as Hume Riverina Community Legal Service's legal professional obligations.

This policy does not relate to Staff Records. For current and former staff members please reference the UMFC Employee Records Privacy Policy for further information.

DEFINITIONS

Personal Information - information or an opinion (including information or an opinion forming part of a database), that is recorded in any form (whether true or not), about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive information - an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

PERSONAL AND SENSITIVE INFORMATION

We ask clients for some personal information to:

- ensure that they receive an appropriate and relevant service
- meet our accountability requirements to government.

Clients have the option of not identifying themselves when entering into transactions with us; however, if personal information is not provided, we may be restricted in our ability to offer a service.

We collect only information that is relevant for providing a particular service or fulfilling a particular function or meeting a legal or regulatory obligation.

Some personal information is sensitive information. Information of this type can be collected only when:

- the person has consented
- the collection is required by law
- it is necessary to prevent or lessen a serious and imminent threat to the life or health of a person and that person is legally incapable or physically cannot communicate consent
- it is necessary for the establishment, exercise or defence of a legal or equitable claim.

THIRD PARTIES

Where reasonable and practicable to do so, we will collect Personal Information only from the person(s) involved. However, in some circumstances we may be provided with information by third parties. In such a case, we will take reasonable steps to ensure that the person(s) involved is made aware of the information provided to us by the third party.

STORAGE OF INFORMATION

Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure.

When Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify Personal Information.

ACCESS TO INFORMATION

In general, access to personal information is limited to:

1. authorised program workers
2. the person about whom the information is held, and
3. with the person(s)' permission, other people.

The person(s) has the right of access to, and correction of, their personal information.

A person may request access to their personal information in writing. This request should include the type of information the person would like access to and their reasons for doing so. A [Personal Information Access Request Form](#) is the preferred option for making this request. If the request is verbal, then a case note will be made and filed within the relevant program or service.

All client files are the responsibility of UMFC, who retains the right to decide on the release of file information to persons as outlined in UMFC Privacy Procedure.

SHARING OF INFORMATION

UMFC supports the sharing of relevant information as part of the Victorian Government Information Sharing Reforms to ensure client safety and enhance client outcomes.

More information about the Child Information Sharing Scheme and the Family Violence Information Sharing Scheme is available through these documents:

- [Child Information Sharing Scheme](#)
- [Family Violence Information Sharing Scheme](#).

Further to the above, UMFC may wish to share information to other relevant services to enhance client outcomes and promote greater continuity and coordination. This sharing would occur with the full knowledge and written consent of the individual or their authorised representative via a [Client Authority to Release Information Form](#).

MAINTAINING THE QUALITY OF PERSONAL INFORMATION

It is important to us that Personal Information is up to date. We will take reasonable steps to make sure that Personal Information is accurate, complete and up to date. If a person(s) finds that the information we have is not up to date or is inaccurate, they should advise us as soon as practicable so records can be updated and UMFC can ensure provision of quality services to clients.

RELATED DOCUMENTS

- Code of Conduct
- Privacy Procedure
- Privacy and Data Breach Procedure
- UMFC Employee Records Privacy Procedure
- HRCLS Information Barrier Policy

RELATED LEGISLATION

- [Privacy and Data Protection Act 2014](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Australian Privacy Principles](#)
- [Information Privacy Act 2000 \(Vic\)](#)
- [Family Violence Information Sharing Scheme \(2018\)](#)
- [Child Information Sharing Scheme \(2018\)](#)

Document No: 1	Version: 1.6	Owner: Quality and Risk	Approved by: EXEC
Date reviewed: June 2025		Date of next review: June 2027	