

Privacy and Confidentiality Policy and Procedure

1. Purpose

CatholicCare Canberra & Goulburn is committed to protecting the privacy and confidentiality of clients, staff, Board members, volunteers and stakeholders in the way information is collected, stored, and used.

This policy provides guidance on CatholicCare's legal obligations and ethical expectations in relation to privacy and confidentiality.

CatholicCare holds two types of information which are covered by this policy, personal and organisational information.

2. Policy Statement

CatholicCare is committed to ensuring that information is used in an ethical and responsible manner and recognises the need to be consistent, cautious, and thorough in the way that information is recorded, stored, and managed.

3. Procedure Information

The privacy of personal information is defined by legislation (Privacy Act 1988). At all times, CatholicCare acts in accordance with these legal requirements which are underpinned by the information below.

CatholicCare provides a range of services directly under contract with Australian or State/Territory Government Agencies or medical bodies. In some circumstances we collect your personal information from these government agencies or medical bodies, who also comply with the Privacy Act.

CatholicCare staff are legally and ethically bound to maintain client confidentiality. Staff affiliated with professional bodies are also required to comply with particular codes of conduct and conditions in relation to client confidentiality.

CatholicCare is also required to comply with other Australian and State/Territory Government Legislation relevant in providing services to you and how your personal information is used.

CatholicCare works with a variety of stakeholders and the organisation may collect confidential or sensitive information about its stakeholders as part of a working relationship. Staff at CatholicCare will not disclose information about its stakeholders that is not already in the public domain without stakeholder consent. The manner in which staff members manage stakeholder information will be clearly articulated in any contractual agreements that the organisation enters into with a third party.

Collection of Information

Personal information collected by CatholicCare is only for purposes which are directly related to the functions or activities of the organisation. These purposes include:

- Enquiry about programs
- Referral to programs
- Providing treatment and support to clients
- Administrative activities, including human resources management
- Sector development activities
- Community development activities
- Fundraising
- Complaint handling
- Fees and Payments

Credit Card Information - CatholicCare's card transactions are fulfilled by an authorised banking institution. When collecting credit card information for online transactions, CatholicCare offers secured server transactions that encrypt your information in transit to help prevent others from accessing it. Your credit card details are encrypted and then removed from our system once your payment has been processed.

CatholicCare provides information to clients on collecting health and personal information including:

- Purpose of collecting information
- How information will be used
- Who (if anyone) information may be transferred to and under what circumstances information will be transferred
- Limits to privacy of personal information
- How a client can access or amend their information
- How a client can make a complaint about the use of their personal information.

Use and Disclosure

CatholicCare only uses personal information for the purposes for which it was given, or for purposes which are directly related to one of the functions or activities of the organisation. It may be provided to government agencies, other organisations, or individuals if:

- The individual has consented
- It is required or authorised by law
- It will prevent or lessen a serious and imminent threat to somebody's life or health.

Data Quality

CatholicCare takes steps to ensure that the personal information collected is accurate, up-to-date, and complete. These steps include maintaining and updating personal information when we are advised by individuals that it has changed (and at other times as necessary), and checking that information provided about an individual by another person is correct.

Data Security

CatholicCare takes steps to protect the personal information held against loss, unauthorised access, use, modification, or disclosure and against other misuse. These steps include reasonable physical,

technical, and administrative security safeguards for electronic and hard copy of paper records as identified below.

Reasonable physical safeguards include:

- Locking filing cabinets and unattended storage areas
- Removing any sensitive business information from your desk every day, including: USB sticks, notebooks, and printed documents.
- Erasing Whiteboards containing sensitive or restricted information after meetings or when no longer in use.
- Physically securing the areas in which the personal information is stored
- Not storing personal information in public areas
- Positioning computer terminals so that they cannot be seen or accessed by unauthorised people or members of the public.

Reasonable technical safeguards include:

- Using passwords to restrict computer access, and requiring regular changes to passwords
- Establishing different access levels so that not all staff can view all information
- Ensuring information is transferred securely (for example, not transmitting health information via non-secure email)
- Using electronic audit trails
- Installing virus protections and firewalls.

Reasonable administrative safeguards include not only the existence of policies and procedures for guidance but also training to ensure staff, Board members and volunteers are competent in this area.

Access and Correction

Individuals may request access to personal information held about them. Access will be provided unless there is a sound reason under the Privacy Act or other relevant law. Other situations in which access to information may be withheld include:

- There is a threat to the life or health of an individual
- Access to information creates an unreasonable impact on the privacy of others
- The request is clearly frivolous or vexatious or access to the information has been granted previously
- There are existing or anticipated legal dispute resolution proceedings
- Denial of access is required by legislation or law enforcement agencies.

Amendments may be made to personal information to ensure it is accurate, relevant, up-to-date, complete, and not misleading, taking into account the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, CatholicCare may refuse the request.

CatholicCare is required to respond to a request to access or amend information within 30 days of receiving the request. However, some requests may take longer to process because of the substantial amount of documents held in respect of some matters.

Where the information is held in security, CatholicCare reserves the right to charge a fee to cover the cost of retrieval and supply of information to you. However, we will endeavour at all times to ensure that the cost of such retrieval and supply is reasonable.

In some circumstances where we are providing services to you under a contract with a government agency or another organisation, it may be more appropriate for you to request disclosure by that government agency or organisation.

Collection, Use and Disclosure of Confidential Information

Other information held by CatholicCare may be regarded as confidential, pertaining either to an individual or an organisation. The most important factor to consider when determining whether information is confidential is whether the information can be accessed by the general public.

Staff members if unsure if information is sensitive or confidential, are to refer to the relevant Director before transferring or providing information to an external source.

Breach of Privacy or Confidentiality

CatholicCare follows the Office of the Australian Information Commissioner's 'Data Breach Notification - A guide to handling personal information security breaches' when handling accidental and unauthorised disclosures of personal information.

If you have concerns that your personal information has been mishandled under the Australian Privacy Principles, CatholicCare asks that you raise your concerns with our privacy contact officer, the Deputy CEO by:

- Telephone on 62954300
- In writing to: Deputy CEO (Privacy Officer) PO Box 3167 Manuka ACT 2603

If a client or stakeholder is dissatisfied with the conduct of a CatholicCare staff or Board member, a complaint should be raised. Information on making a complaint will be made available to clients, stakeholders and will be found on the CatholicCare website.

If staff are dissatisfied with the conduct of a colleague with regards to privacy and confidentiality of information, the matter should be raised with the staff member's Manager or Director. Staff members who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action.

Direct Marketing

CatholicCare may from time to time use your personal information such as your address or contact details to provide you with information about other services we offer.

If at any time you do not wish to receive any information about these services, please feel free to contact us on 02 62954300 and we will not send you any further material.

CatholicCare will not disclose your personal information to any party outside the organisation except for the purposes of furthering your services, or as a requirement under Australian Law.

Changes to this Policy

This policy is developed in consultation with key staff and approved by the Deputy CEO. This policy is to be part of all staff orientation processes and all employees are responsible for understanding and adhering to this policy.

This policy will be reviewed in line with CatholicCare’s quality improvement program and/or relevant legislative changes.

4. Definitions

Privacy provisions of the Privacy Act 1988 govern the collection, protection and disclosure of personal information provided to CatholicCare Canberra & Goulburn by clients, Board members, volunteers and stakeholders.

Confidentiality applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those authorised to have access and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature, e.g., it is information that is not available in the public domain.

Consent means voluntary agreement to some act, practice, or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.

Individual means any person such as a client, staff member, Board member, volunteer, contractor, or a member of the public.

Organisational information includes publicly available, and some confidential, information about organisations. Organisational information is not covered in the Privacy Act (1988), but some organisational information may be deemed confidential.

Personal information means information or an opinion (including information or an opinion forming part of a database) about an individual (Office of the Federal Privacy Commissioner, 2001). It may include information such as names, addresses, bank account details and health conditions. The use of personal information is guided by the Federal Privacy Act (1988).

The public domain in relation to confidentiality is “common knowledge,” i.e., information that can be accessed by the general public.

5. Responsibilities

Human Resources

Deputy CEO

Chief Financial Officer

6. Key Performance Indicators

CatholicCare provides quality services in which information is collected, stored, used, and disclosed in an appropriate manner complying with both legislative requirements and ethical obligations.

All staff and Board Directors understand their privacy and confidentiality responsibilities in relation to personal information and organisational information about CatholicCare, its clients, staff, and stakeholders. This understanding is demonstrated in all work practices.

All information that is gathered is stored securely, either electronically or manually via secure filing cabinets.

Effective Date: March 2022