CatholicCare
DIOCESE OF BROKEN BAY

Agency Privacy and Confidentiality

Policy

Version: 10.0
Updated: 23 March 2026
Review due: March 2027
Document ID: 10011-062

Contents

Introduction 3
Purpose 3
Scope 3
Policy Statement 3
Application of the Australian Privacy Principles 4
- Information collection & informed consent 4
- Storage & security 5
- Confidentiality 5
- How we use information 5
- Direct Marketing 6
- Access to and amendment of information 6
- Disclosure 7
- Identifiers and anonymity 7
- Overseas disclosure of personal information 8
- Disposal of information 8
- Data / privacy breaches 8
- Access to Privacy Policy 10
- Registers 10

Privacy Officer 10
Concerns or complaints 10
Related documents 11
- Policies and practice guidelines 11
- Forms and resources 11

External resources 12
Glossary 12
Sign off and review 13
Revision history 13

Introduction

CatholicCare Diocese of Broken Bay (CatholicCare) respects the rights of all individuals to have their personal and sensitive information collected, maintained, and managed in a way that ensures privacy and confidentiality.

CatholicCare's Privacy Policy is underpinned by the following State and Federal legislation:

- Privacy Act 1988 (Cth) – setting out the Australian Privacy Principles (APP) and the Notifiable Data Breaches Scheme
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- Privacy and Personal Information Protection Act 1988 (NSW) (PPIPA Act)– setting out the Information Privacy Principles (IPP)
- Health Records and Information Privacy Act 2002 (NSW) (HRIP Act) – setting out the Health Privacy Principles (HPP)
- Government Information (Public Access) Act 2009 (GIPA Act)
- Surveillance Devices Act 2007 (NSW)

CatholicCare is also required to comply with a number of industry standards which create obligations in relation to the protection of the privacy and confidentiality of personal information.

Purpose

This policy identifies how personal information will be collected, stored, used, disclosed, and disposed of by CatholicCare. We also outline how staff and clients can access and amend their personal information and what steps we will take in the event of a data breach.

Scope

This policy applies to all staff, contractors, foster carers, volunteers and students.

Policy Statement

Information and data collection is a requirement of many CatholicCare funding contracts with Government. It is important for CatholicCare to collect a range of personal information to ensure that we provide quality services that are tailored to an individual client's needs. We also use data for the purpose of research undertaken to improve the quality and types of service. In addition, staff personal data is collected for the purposes of employment records, payroll processing and compliance checks.

CatholicCare is committed to ensuring that personal information held by CatholicCare is protected from misuse, interference, unauthorised access, modification, or disclosure. CatholicCare will also take steps to safeguard information when it is no longer required, through destruction or de-identification.

CatholicCare will only collect and use personal information where:

- It is for a lawful purpose directly related to providing services, and

- It is reasonably necessary for us to have this information.

CatholicCare only collects personal information where:

- The client has consented and/or
- Collection is required by law and/or
- It is needed to deal with a serious and imminent threat to any person or to the general public (and the person is incapable of giving consent).

CatholicCare will implement practices, procedures, and systems to ensure compliance with privacy obligations including developing personal information security measures to:

- **PREVENT** the misuse, loss, unauthorised access to or disclosure of personal information, including identifying and assessing security risks.
- **DETECT** privacy breaches promptly.
- **RESPOND** to potential privacy breaches in a timely and appropriate manner.

CatholicCare will ensure that managing the security and privacy of personal information of its clients and staff is sufficiently resourced and managed, and staff are adequately trained, to foster a privacy and security aware culture across the agency.

CatholicCare recognises that Information Communication Technology (ICT) security of both hardware and software is a critical element of ensuring the privacy of personal information across the agency and so we will implement effective internal and external security measures to minimise the risk of a breach of privacy through inappropriate access to CatholicCare's ICT systems. This will include back up of essential information systems, and assessment of the effectiveness of security controls in place in relation to any third-party providers (cloud systems).

Application of the Australian Privacy Principles

CatholicCare is committed to the protection of personal privacy in accordance with legislative and regulatory obligations.

Information collection & informed consent

CatholicCare will only collect information directly from the client, or from a third party if the client consents, or from a legally recognised or appointed representative. The client, or their legally recognised representative, must provide informed consent before personal information can be collected and disclosed.

If a child is under 16 years of age and it is not reasonable or practicable to collect the information directly from them, the information may be collected from a parent or guardian without the child's consent.

Collection will not be intrusive or excessive. CatholicCare will endeavour to collect information that is relevant, accurate, up-to-date, and complete.

CatholicCare clients will be informed of the following:

- The fact that information is being collected,
- Whether the collection is required by law,
- Who will hold/receive the information,

- The purposes for which information is collected, which may include how the information is relevant to the services to be provided and whether information is required to be submitted to Government agencies. If so, the nature of the information to be provided,
- The consequences of not providing the information,
- How the client can access the information and make changes if it's not accurate, and
- How they can make a complaint about any privacy concerns.

CatholicCare will require clients to complete a *Personal Information Collection Notice and Consent Form* to give consent to the collection, storage and use of their personal information.

If CatholicCare receives unsolicited personal information about a person, we will determine whether the information is reasonably necessary for CatholicCare to carry out its services and functions. If the information is not necessary, it will be destroyed as soon as possible unless it is part of a government record or it is unlawful to do so. If information is received orally, notes of the information will not be made and kept unless the information is necessary for CatholicCare to carry out its services and functions.

Applicants for employment will be provided with a *Personal Information Collection Notice for Employment Purposes* early in the recruitment process.

Storage & security

CatholicCare will ensure all personal information is kept safely and securely to prevent loss, unauthorised access, use, modification or disclosure or other misuse. Information will not be made available to any unauthorised party.

Confidentiality

CatholicCare staff will be trained in confidentiality requirements and exceptions. Staff and contractors are under obligation to not access, use, disclose or keep personal information except in performing their work or contract engagement.

How we use information

Clients

CatholicCare will only use the personal information of clients for the purpose it was collected, unless:

- The client gives their express written consent to the information being used for other purposes,
- Further use of the information is directly related to the primary purpose of the original collection,
- Further use of the information is necessary to prevent a serious and imminent threat to the life or health of any individual or to public health and safety,
- The use is required or allowed to be made by Australian law or a court/tribunal order, or
- The use is reasonably necessary for law enforcement purposes or the protection of the public revenue.

Staff, contractors, and volunteers

Personal information of staff, contractors, and volunteers will be used as follows:

- Assessing the suitability of an applicant to the position for which they have applied,
- Administering an individual's employment or contract,
- Rostering and shift attendance,

- Insurance purposes,
- Fulfilling our functions and activities (including seeking funding, and to meet contractual and compliance obligations with funding bodies or regulatory bodies),
- Work health safety obligations, and
- Satisfying legal obligations, e.g., child protection and safeguarding legislation.

Direct Marketing

Fundraising appeals (mail, email, SMS, phone, digital campaigns) are a form of direct marketing.

Personal information will only be used to communicate directly with an individual to seek donations or support when:

- The personal information was collected directly from the individual,
- The individual would reasonably expect it to be used for fundraising
- Each communication includes a simple opt-out mechanism, and
- The individual has not previously opted out.

For further information see *Fundraising & Donations Policy*.

Access to and amendment of information

Clients

CatholicCare will take reasonable steps to enable clients to find out:

- Whether we hold their personal information,
- What type of information we hold about them,
- The purposes for which the information will be used, and
- How they can access the information.

Individuals seeking to access or amend information should do so in writing to the Privacy Officer; by completing the *Application for Access to Information Form* or the *Application for Amendment of Personal or Health Information Form*. Further information about this process can be provided to the client in the *Information Sheet: Application for Access to Information*.

If a client requests access to their personal information, it will be provided without unreasonable expense or delay, unless:

- This would pose a serious and imminent threat to the life, health or safety of any individual,
- This would unreasonably affect the privacy of other individuals,
- The information is related to existing or anticipated legal proceedings between the organisation and the client and this information could not be obtained by the legal process of discovery in those proceedings,
- It would be unlawful to provide access,
- Denying access is required or authorised by law, or
- Providing access would be likely to prejudice an investigation into possible unlawful activity.

If we deny access to personal information, reasons will be provided in writing for doing so, within 14 days of the date of when the application has been submitted.

We will allow clients to apply to update, correct or amend their personal information, to ensure its accuracy. If CatholicCare is not prepared to amend the information, the client will be informed of the reasons for the refusal. If requested, CatholicCare will take reasonable steps to attach a statement by the client to the original information to detail the amendment sought or state that the client believes the information held is inaccurate, incomplete, not up-to-date and/or misleading.

Staff

If a staff member wishes to access their personnel file (paper or electronic), then they can do so under supervision or 'read-only' access.

If a staff member feels that anything in their personnel file is false or inaccurate, then they may make an official written request to have the records removed or amended, stating specific reasons for doing so. The Executive Manager People & Culture will review the member's request and ensure that only factual and true representations of events and processes are retained in the staff member's personnel file.

If a staff member is still not satisfied with the content of his or her personnel file, then they should follow the *Resolving Workplace Issues (Staff Grievance) Policy*.

Disclosure

CatholicCare will only disclose personal information:

- For the primary purpose for which it was collected, or
- For a directly related secondary purpose within reasonable expectations as a client, or
- With a client's consent, or
- To deal with a serious and imminent threat to personal or public health or safety, or
- Where authorised or required by law. This includes CatholicCare's obligations to respond to a subpoena to produce documents, or other Court Order. Where CatholicCare is concerned that the production of documents in response to a subpoena may create a significant risk to the client or another person, or where the subpoenaed documents include documents in respect of which CatholicCare may have a legitimate reason for objecting to production (e.g., Family Court Counselling) we will seek advice as to the appropriate course of action.

CatholicCare will only disclose sensitive personal information:

- With a client's written consent, or
- To deal with a serious and imminent threat to personal or public health or safety, or
- Where authorised or required by law.

Identifiers and anonymity

CatholicCare will use unique identifiers in our client management systems. CatholicCare will not use a government-issued identifier that has been assigned to an individual for its own use unless it`s use is required by Australian law or a court/tribunal order.

Individuals will be told if it is lawful and practicable to use a pseudonym when they are dealing with CatholicCare. In these types of instances, their ability to fully participate may be limited if they cannot be identified or do not allow us to collect certain personal information.

Overseas disclosure of personal information

CatholicCare uses secure cloud-based systems and service providers that may store or process personal information outside Australia, including in the United States. Where personal information is disclosed to overseas recipients, we take reasonable steps to ensure that those recipients handle the information in accordance with the Australian Privacy Principles (APPs), including through contractual obligations, due diligence of their privacy and security practices, and technical safeguards. In some circumstances, an overseas recipient may be subject to laws that differ from Australian privacy laws; however, we remain accountable for the protection of personal information as required under APP 8.

CatholicCare will only disclose personal information outside Australia where one or more of the following applies:

- the overseas recipient is subject to a law or binding scheme that is substantially similar to the Australian Privacy Principles and/or Health Privacy Principles, and individuals have enforceable rights or mechanisms to protect their information; or
- the client or staff member has provided express written consent; or
- the disclosure is necessary for the performance of a contract with, or directly in the interests of, the client or staff member; or
- the disclosure will benefit the client or staff member, it is impracticable to obtain consent, and CatholicCare reasonably believes the individual would be likely to give consent; or
- the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of any person, or to public health or safety; or
- the disclosure is required or authorised by Australian law or a court or tribunal order.

Disposal of information

CatholicCare as care provider will only collect personal information for the purposes of providing services to clients and to perform its functions, including service evaluation and quality improvement.

Personal information will be disposed of in accordance with the timeframes set out in relevant legislation and the requirements of the funding agency. Refer to *Records Management Policy*, *Archiving Practice Guidelines* and individual program guidelines.

Personal information is destroyed securely in accordance with relevant legislation and the requirements of the funding body.

Data / privacy breaches

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations to respond appropriately to any data breach.

An eligible data breach can involve:

- Unauthorised access to personal information,
- Unauthorised disclosure of personal information; or
- Loss of personal information where it is likely to result in unauthorised access or disclosure and that access, disclosure or loss is "**likely to result in serious harm to any of the individuals to whom the information relates**".

Where a privacy data breach is known to have occurred (or is suspected) any member of CatholicCare staff who becomes aware of this **must immediately report it to the Privacy Officer** who is the Executive Manager Quality Safeguarding Risk and Compliance. This must happen as soon as possible but at least within 24 hours. The CatholicCare Privacy Officer or their delegate will notify the Executive Director and may notify the Diocesan Privacy Officer, depending on an assessment of the scale and potential impact of the breach. The Chief Information Officer will also be notified if the breach involves digital data within our information systems.

The Information that should be provided (if known) at this point includes:

- When the breach occurred (time and date),
- Description of the breach (type of personal information involved),
- Cause of the breach (if known) otherwise how it was discovered,
- Which system(s) if any are affected?
- Which department/area is involved? and
- Whether any corrective action has occurred to attempt to remedy the breach (or suspected breach).

The *Data Breach Internal Notification Form* can assist in documenting the required information.

In some instances, CatholicCare has an obligation to notify both the individual and the Government if a data breach has occurred which causes personal information to be compromised. CatholicCare will assess any suspected data breach to determine:

- Whether there been unauthorised access, unauthorised disclosure, accidental loss or theft of personal information the agency holds,
- Whether it is likely to result in serious harm to the individual(s) whose data has been breached,
- What actions will need to be taken to remedy the breach, and
- Whether it is necessary to notify the breach to the Office of Australian Information Commissioner (OAIC) and any affected individuals.

Where an eligible data breach has occurred, the Privacy Officer will complete the OAIC online *Notifiable Data Breach Form*, and notify the individuals affected as per the Notifiable Data Breaches Scheme.

If CatholicCare has taken appropriate steps to mitigate the breach, and this action was successful in preventing a likely risk of serious harm then notification may not be required. The Incident Coordination Committee (ICC) can be called to review all data breaches to ensure there is an adequate response to the data breach, that any notification requirements have been met, that the circumstances of the breach and response are well documented and that any systemic issues contributing to the data breach have been identified and addressed.

In every instance, CatholicCare will respond to a data breach or suspected data breach with the following steps:

Step 1: Contain the breach and conducting a preliminary assessment.

Step 2: Evaluate the risks associated with the breach.

Step 3: Implement mitigation strategies to prevent risk of serious harm to individual/s.

Step 3: Assess and determine whether the OAIC and/or any affected individuals need to be notified.

Step 4: Make any required notification. –.

Step 5: Take action to prevent future breaches.

See *Data Breach Practice Guidelines* for further details

Access to Privacy Policy

CatholicCare will provide client access to our Privacy and Confidentiality Policy and our Privacy & Confidentiality Statement on our website *https://www.catholiccaredbb.org.au* and a paper version (uncontrolled) is available at all CatholicCare services. Program and operation leaders are responsible for ensuring program relevant privacy information is provided directly to clients, and clients are supported to understand their rights in relation to privacy.

If copies of these documents are requested in a different format, CatholicCare will take reasonable steps to provide the person or body with a copy in the form requested.

Registers

CatholicCare will maintain registers to keep a record of:

- Complaints about breaches of privacy,
- Data breaches, and
- Requests for access to or amendment of client or staff files or records.

Privacy Officer

All requests for access to or amendment of information, complaints about breaches of privacy and confidentiality, and data breach concerns will be directed to the Privacy Officer. The Privacy Officer for CatholicCare is the Executive Manager Quality Safeguarding Risk and Compliance.

Concerns or complaints

Complaints about privacy or a breach of the Australian Privacy Principles are taken seriously and are handled in accordance with CatholicCare *Complaints and Feedback Policy* and *Managing Complaints Practice Guidelines*. If a client or staff member has concerns about the way their personal information has been handled, we ask that you try to resolve your information or privacy complaint directly with us first.

You can do this by contacting:

The Privacy Officer
Executive Manager Quality Safeguarding Risk and Compliance
CatholicCare Diocese of Broken Bay
P: (02) 9481 2600
E: info@catholiccaredbb.org.au
If you are unhappy with CatholicCare's response, you can contact one of the following:

Information and Privacy Commission NSW

The Information and Privacy Commission NSW (IPC NSW) has complaint handling responsibilities under the *Government Information (Information Commissioner) Act 2009,* the *NSW Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *NSW Health Records and Information Privacy Act 2002* (HRIP Act) including private agencies, like CatholicCare, which provides contracted services to the community on behalf of the NSW government.

Complaints can be lodged with the Information Commissioner:
P: 1800 IPC NSW (1800 472 679)
E: ipcinfo@ipc.nsw.gov.au
W: https://www.ipc.nsw.gov.au/

Office of the Australian Privacy Commissioner

The Office of the Australian Information Commissioner (OAIC) has complaint handling responsibilities under the *Privacy Act 1988 (Cth)* (Privacy Act). You can complain to the OAIC if you believe that your privacy has been interfered with by an Australian government agency or a private sector organisation, like CatholicCare, covered by the *Privacy Act 1988 (Cth).*

Privacy complaints can be lodged via:
P: 1300 363 992 (Enquiries only)
W: https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us
A: GPO Box 5288, Sydney NSW 2001

Related documents

Policies and practice guidelines

- *Acceptable Use of IT Facilities Policy*
- *Archiving Practice Guideline*
- *Client Services Charter*
- *Complaints and Feedback Policy*
- *Data Breach Practice Guidelines*
- *Information Security Policy*
- *Managing Complaints Practice Guidelines*
- *Records Management Policy*
- *Subpoena Practice Guideline*

Forms and resources

- *Application for Access to Information Form*
- *Application for Amendment of Personal or Health Information Form*
- *Information Sheet: Application for Access to Information*
- *Data Breach Internal Notification Form*
- *Personal Information Collection Notice and Consent Form*
- *Personal Information Collection Notice for Employment Purposes*
- *Privacy and Confidentiality Statement*
- *Your Privacy Brochure*

External resources

- *Australian Privacy Principles*
- *Information and Privacy Commission NSW*
- *NSW Government Information (Information Commissioner) Act 2009*
- *NSW Health Records and Information Privacy Act 2002 (HRIP Act)*
- *NSW Privacy and Personal Information Protection Act 1998 (PPIA Act)*
- *Office of the Australian Information Commission – Guide to securing personal information*
- *OAIC: Data Breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*
- *OAIC: Report a Notifiable Data Breach*
- *Privacy Act 1988 (Cth)*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*

Glossary

Clients

Clients is the term used for all recipients of CatholicCare services. It includes NDIS participants, young people and children.

ICC

Incident Coordination Committee

ICT

Information Communication Technology

OAIC

Office of the Australian Information Commissioner

Personal Information

Refers to information or an opinion, whether true or not, about an individual whose identity is apparent or could be reasonably ascertained from that information or opinion.

Sensitive Personal Information

Includes ethnic or racial origin; political opinions; membership of a political association; religious or philosophical beliefs or affiliations; membership of a professional or trade association; health; sexual preferences, practices or activities; and criminal record.

Sign off and review

This document remains valid until it is either superseded by a new version or officially revoked.

CatholicCare values your input and welcomes feedback on this policy. Your suggestions help us improve and better support your work. Please send any feedback to policy.updates@catholiccaredbb.org.au.

Version	Authorised by	Approved date	Review cycle	Review due
10.0	Executive Manager Quality Safeguarding Risk and Compliance	23 March 2026	1 year	23 March 2027

Revision history

Version	Description	Author	Amendment date
10.0	Reviewed against APP and updated where required	Policy Specialist	23 March 2026