Privacy and Confidentiality

Mandatory Guidelines

catholic care

WESTERN SYDNEY AND THE BLUE MOUNTAINS

STATEMENT

Catholic Care is committed to protecting the privacy and confidentiality of clients, employees, and any other stakeholders in the way that information is collected, stored and used.

This document provides guidance on legal obligations and ethical expectations in relation to privacy and confidentiality and has been developed in line with the privacy principles in the legislation including:

- Federal Privacy Act 1988 and the Privacy Amendment (Private Sector) Act 2000;
- Privacy and Personal Protection Information Act 1998 (NSW);
- Health Records and Information Privacy Act 2002 (NSW).

This document outlines how Catholic Care collects, uses, stores, disseminates and disposes of personal information.

Catholic Care ensures that procedures are in place to demonstrate that decisions and actions relating to privacy and confidentiality comply with federal and state laws.

It is a condition of Catholic Care contracts/agreements that the Privacy and Confidentiality guideline is read and agreed to prior to commencing work/placement. All employees are provided with ongoing support and information to assist them to establish and maintain privacy and confidentiality.

SCOPE

This guideline applies to all clients, employees and stakeholders of Catholic Care. Paid employees, students, volunteers and contractors must comply with the Catholic Care Privacy and Confidentiality guideline in regard to obtaining and protecting personal information.

Catholic Care collects personal information, including health information and other sensitive information about:

- Clients, employees, stakeholders, contractors and job applicants
- Other people who come into contact with the Catholic Care

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

- As required by the funding body to provide requested services
- To administer employment processes and contracts
- To provide a safe working and learning environment
- To discharge the Catholic Care's legal obligations
- For insurance purposes

In collecting personal information, Catholic Care:

- informs why personal information is collected and to whom else it may be disclosed.
- collects sensitive information, such as health information, with consent unless necessary to prevent harm to life or health.
- collects personal information directly unless it is a minor, under guardianship or has given consent for someone else to provide the information.
- will ensure that personal information held is accurate, up-to-date and complete.

- will protect personal records from loss, unauthorised access, misuse, modification and disclosure and will ensure its appropriate disposal.
- will provide access to records upon a written request.
- will allow people to correct any wrong, incomplete or misleading personal information held.
- will not use personal information for any other purpose except with consent, unless necessary to prevent harm to life or health.
- will not disclose personal information to any other person or organisation without consent unless necessary to prevent harm to life or health.
- only use identifying codes where necessary.
- will take all reasonable steps to de-identify health/personal information before it is disclosed for data collection or research purposes
- staff will only access records linked to their work where necessary or of clients they are directly working with.

Catholic Care will adhere to all relevant legislation. Information protected by the relevant legislation includes:

- Personal information. This is information or an opinion, whether true or false and whether or not recorded in material form, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion. This is information or an opinion about a person's:
    - Racial or ethnic origin
    - Religious beliefs or affiliations
    - Philosophical beliefs
    - Membership of a professional or trade association
    - Sexual preferences or practices
    - Criminal record
    - Health information including disabilities

DEFINITIONS

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.

Consent - a voluntary agreement to some act, practice or purpose.

Data Breach - When personal information held by an organisation is disclosed accidentally, lost, or accessed without permission. This can be as a result of human error, or through malicious action by an employee or an external party.

Examples include where a secure IT system containing personal information has been hacked, a storage device being lost by an employee, or an employee accidentally releasing personal information to the wrong person.

Individual - any person such as a client or employee.

Organisational information - includes publicly available, and some confidential, information about organisations.

Personal information - 'Information about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.'

Personal information includes a person's health information, tax file number, and information about racial or ethnic origin, sexual orientation or criminal record.

Privacy Amendment (Private Sector) Act 2000 amended the Privacy Act 1988 to regulate some organisations in the private sector

Privacy and Personal Information Protection Act 1998 (NSW) - contains a set of privacy standards called Information Protection Principles that regulate the way NSW public sector agencies handle personal information (excluding health information).

Privacy provisions of the Privacy Act 1988 - govern the collection, protection and disclosure of personal information provided to Catholic Care by clients, employees and stakeholders.

Public domain - in relation to confidentiality is considered "common knowledge," e.g. information that can be accessed by the general public.

Record - any document or other source of information complied, stored or recorded in written form or on film, or by electronic process or by any other manner or means.

PRINCIPLES & RESPONSIBILITIES

Catholic Cares ensures that:

- Information is used in an ethical and responsible manner
- It operates in a consistent, cautious and thorough manner in the way that information about clients, employees and stakeholders is recorded, stored and managed
- All individuals including clients, employees and stakeholders have legislated rights to privacy of personal information
- All employees and stakeholders are to have an appropriate level of understanding regarding how to meet the organisation's legal and ethical obligations to ensure privacy and confidentiality

All employees and stakeholders of Catholic Care have a responsibility to ensure Privacy and Confidentiality.

The following outlines the responsibilities of the Executive Director, Management, and other employees relating to privacy and confidentiality:

Executive Director

- Endorse Privacy and Confidentiality Policy
- Be familiar with the organisation's legislative requirements regarding privacy and the collection, storage and use of personal information
- Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to the Organisation, its clients, employees and stakeholders
- Comply with Privacy and Confidentiality Policy and associated procedures

Executive Team, Senior Management and Management

- Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information

- Understand Catholic Care's ethical standards with regards to the treatment of other confidential information relating to clients, employees, and stakeholders
- Ensure systems are in place across the organisation to adequately protect the privacy of personal information and confidentiality of other sensitive information
- Act in accordance with Catholic Care processes in place to protect privacy and confidentiality
- Comply with the Privacy and Confidentiality Policy and associated procedures

Employees of Catholic Care

- Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information
- Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to clients, employees and stakeholders Act in accordance with Catholic Care processes in place to protect privacy and confidentiality
- Should only access personal or sensitive information which is relevant to their role; accessing of information outside work requirements is subject to disciplinary action including immediate termination
- Comply with Privacy and Confidentiality Policy and associated procedures

DATA & SECURITY

Catholic Care 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 advised by individuals that it has changed (and at other times as necessary).

Catholic Care 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 records as identified below.

Physical safeguards include:

- Locking filing cabinets and unattended storage areas
- 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

Technical safeguards include:

- Using passwords to restrict computer access, and requiring regular changes to passwords
- Establishing different access levels so that not all employees can view all information
- Ensuring information is transferred securely (for example, transferring sensitive information via a secure email)
- Printing documents with the secure printing feature
- Installing virus protections and firewalls

PROCEDURE

Client records

Client records will be confidential to clients and to paid employees, students, volunteers and contractors.

All client records will be kept securely electronically in an approved Electronic Document Record Management System (EDRMS) and/or as physical files that are stored on site and securely locked and inaccessible to anyone without specific authorization. Client records will be updated, archived and destroyed according to the organisation's client records guidelines.

Personnel files

A personnel file is held for each staff member and contains:

- contact details and contact details in case of an emergency
- a copy of the employee's contract
- all correspondence relating to job description changes, salary changes, leave entitlements such as long service leave, continuous service leave, unpaid and parental leave

Access to personnel information is restricted to:

- the individual staff member accessing their own file
- Human Resources

Corporate records

Corporate records are those that contain confidential or commercially sensitive information about the organisation's business. They include:

- The financial accounts and records
- Taxation records
- The corporate key and other access or user name information
- Records of staff or other internal meetings
- Project management files
- Contracts between the organisation and other parties

Access to these records is limited to Executive Director, the Executive Team, and Advisory Council members.

Requests for access – general records

All records and materials not falling into the categories above may be released to the public at the discretion of the Executive Director.

Any request for access to information should be directed to the Executive Director, who will:

- make available to staff or Advisory Council members information that they are entitled to access
- refer any request from Catholic Care members or the public for access to the organisation's records or materials to the Executive Director.

In considering a request, the Executive Director will take into consideration:

- a general presumption in favour of transparency
- the business, legal, and administrative interests of Catholic Care, including commercial confidentiality and privacy obligations

Where an external party requests access to information that requires staff to devote time to collating, copying or otherwise making material accessible, the Executive Director may determine a fee to be charged.

Requests for access - client records

All clients have the right to access their records and advise Catholic Care about inaccuracies. Clients can request access to their information under the Health Records and Information Privacy Act 2002 (HRIP Act).

To request their client record, requests must:

- be in writing via post or email

Postal Address:	Email:
Level 2, 10 Victoria Road	privacy@ccss.org.au
Parramatta, NSW, 2150	

- include client name and address
- identify the specific information being requested
- specify how they would like to access their information (for example, if they want a copy of it or just to look at the information at their office)
- if they want someone else to access the health information on their behalf they will need to put the name of the person/organisation they are are authorising to access their information.

Upon receiving the request for information, Catholic Care will write to the client with its decision within 45 calendar days from receiving the request. Catholic Care is entitled to charge a fee for providing access to client information.

Requests for information about clients from outside agencies or individuals will be referred to the Program Manager. Before any information is released, Program Manager will contact the client concerned to obtain consent.

In some instances, it may be appropriate or necessary for Catholic Care to refuse clients access to their records in certain circumstances, or restrict access to part of the records only, where providing access to the records would:

- Be unlawful (refer to any relevant legislation in your jurisdiction);
- Pose a serious and imminent threat to the mental health or life of an individual;
- Have an unreasonable impact on privacy of others (for example where services are provided to couples, families or groups);
- Be frivolous or vexatious;
- Be prejudicial to an investigation or prosecution of alleged unlawful activity

Request for access – personnel records

Employees may request access to personal information held about them. Access will be provided unless there is a sound reason under the Commonwealth Privacy Act 1988, the Privacy and Personal Information Protection Act 1998 or another relevant law.

Employees may request their personal information by submitting a written request (via post or email) to Human Resources.

Appeals

Individuals who are refused access to their own records or information files may appeal by contacting the Senior Manager of Clinical Practice who will review the decision in the context of this policy.

The client may also contact the NSW Privacy Commissioner:

- when they are dissatisfied with the response from Catholic Care
- when they believe Catholic Care is charging too much for access to their client information
- when Catholic Care does not respond within 45 days

Clients can contact the NSW Privacy Commissioner with concerns in writing by email, letter or fax. Clients have six months to do this from when they become aware of the situation

DATA BREACH

Catholic Care is committed to protecting the privacy and personal information that it holds about individuals. Catholic Care will act appropriately and in a timely manner in the event of a data breach, to contain the possible resulting harm and notify individuals affected as required. Catholic Care endeavors to prevent data breaches of confidential information.

Data breaches can occur in several ways. Some examples include:

- lost or stolen laptops, storage devices, or paper client records
- hard disk drives and other digital storage media being disposed of or returned to equipment lessors without information being correctly destroyed
- databases being 'hacked' or otherwise illegally accessed
- paper records stolen from unsecured recycling or garbage bins or from cars
- mistakenly providing personal information to the wrong person
- an individual deceiving an agency or organisation into improperly releasing information.

The Notifiable Data Breaches (NDB) scheme (Part IIIC of the Privacy Act) came into effect from 22 February 2018.

The NDB scheme introduces an obligation to notify individuals whose personal information is involved in an eligible data breach. This must include recommendations about the steps individuals should take in response to the breach.

Under the NDB scheme, an eligible data breach occurs if:

- there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an organization or an entity; and

- the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

Data Breach Procedure

If a data breach is suspected to have occurred, the NDB scheme allows a period of 30 days in which an organisation can conduct an assessment to determine if an eligible data breach has occurred.

If an eligible data breach is identified, Catholic Care will notify the Office of the Australian Information Commissioner (OAIC) and follow the requirements under the NDB scheme. The Executive Director must also notify the department as specified in clause 20.6 and clause 24.1 of the contract.

Further information regarding identifying eligible data breaches and determining serious harm is available on the OAIC website.

Identify

When staff have reason to believe there has been a data breach, they should inform the Senior Manager of Clinical Practice immediately.

At this time, details such as when and how the breach was discovered, and by whom, should be recorded. This will be recorded in a Data Breach Incident Reporting form.

Contain

As soon as a breach or suspected breach has been identified, any steps to contain or limit the potential harm should be taken. This may include shutting down a system that has been breached, or recovering any records.

The staff member who discovers the breach will complete a preliminary assessment of the breach and take any immediate action to contain the breach if possible.

Assess

If the preliminary assessment finds that further investigation and assessment is necessary to understand the nature and extent of the breach, it will be escalated to the data breach response team, led by the Senior Manager of Clinical Practice. The team will work together to gather information, assess risks and the likelihood of serious harm from the breach, and therefore whether it is an 'eligible' (notifiable) breach.

To evaluate whether a known data breach is notifiable, consider the following three questions:

- Has there been unauthorised access, unauthorised disclosure, accidental loss, or theft of personal information that the organisation holds?
- For example, the organisation's database is hacked, a portable storage device containing personal information is lost, or the organisation accidentally releases personal information to the wrong person.
- Is it likely that this may result in serious harm to individual/s whose data has been breached?

This can include but is not limited to psychological, financial, emotional, physical or reputational harm. To be able to accurately assess the likelihood and seriousness of harm, it requires looking at the context of the data and how it may have been breached.

For information about the factors to consider when deciding whether harm is likely and/or serious, refer to section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017

- Does the likelihood of serious harm remain despite taking available remedial action?

The obligation to notify the OAIC can be avoided if the organisation takes remedial action in a timely manner to prevent the risk of harm occurring, either by making the harm unlikely to occur, or non-serious.

If the answer to the above three questions is yes, then the breach classifies as an eligible data breach and organisations are required to notify the OAIC and any affected individuals.

If there are reasonable grounds to suspect that there has been a data breach, the data response team should conduct an assessment of the suspected breach. The assessment of a suspected breach must take place within 30 days of it occurring, and should seek to find out the likelihood of serious harm occurring as a result of the suspected breach. If it is assessed to be likely, this has the same notification obligations as a known data breach under the NDB Scheme.

Take remedial action

Remedial action can be taken at any point throughout the data breach response process – the sooner the better. However, it may be that the full extent and nature of the breach, and therefore the actions that could be taken, are not known until after assessing and investigating the breach.

Examples of remedial action include remotely deleting sensitive information from a laptop which has been lost, or emailing affected individuals with advice to change their password details for an online account for which login information may have been hacked.

The data breach response team should document the process of any remedial action, making sure to document rationale and reasoning as to why a certain conclusion has been made.

If, after the remedial action has been taken, the risk of harm is reduced so that it is unlikely to occur, or non-serious, then there is no requirement to notify.

Even if there is no requirement, however, the data response team should consider whether to contact affected individuals with advice for further protecting their information as a customer service measure.

Notify

Once a breach has been assessed as eligible, relevant individuals and bodies should be notified as soon as practicable. Notification must include the following information as a minimum:

- The organisation's name and contact details
- Description of the data breach
- Type of information involved in the breach
- Advice and recommendations for individuals to take in response

1. The OAIC

Senior Manager of Clinical Practice is responsible for notifying and liaising with the OAIC for data breaches which have been assessed as eligible for the purposes of the Notifiable Data Breaches Scheme, using the OAIC's Notifiable Data Breach form.

2. Notification of individuals who are at likely risk of serious harm due to the data breach

   The way notification occurs will depend on the context and nature of the breach, and the relationship of the individuals affected to the organisation. It should occur as soon as practicable after completing the notification statement for the OAIC.

   Notification to affected individuals may contain an explanation of what happened to their personal information, an apology, description of what measures have been put in place as a result of the breach, and advice on what they can do to further protect their information.

Record and review

Data breach log

A data breach log will record all instances of data breaches or suspected breaches, as well as document assessments of the breach and any changes made as a result of a breach.

All staff should be made aware of the log, and Senior Manager of Clinical Practice will be responsible for ensuring that all breaches or suspected breaches are recorded accurately in the log.

Review

Whether or not the breach or suspected breach was notifiable, a review should be conducted into processes relating to the breach to strengthen protections in the future. Depending on the type and seriousness of the breach, this may include:

- A full investigation into how the breach occurred
- Implement measures to ensure it does not reoccur, documented in a prevention plan
- Reviews of security, cybersecurity and ICT policies and procedures
- Audit of implementation of relevant policies and procedures
- Additional staff training about privacy and data breach responses

Approved	10/10/2022 by the Document Endorsement Committee
Next Review	10/10/2024
Version	1.0
Location	H:\1 Policies and Procedures