Access, Use and Security of Records

CATHOLIC ARCHDIOCESE OF PERTH

CAP Policy Register	Information Management
Category	CAPAC Chief Executive Officer
Approving Authority	16 December 2020
Approval Date	First Review: December 2021
Review Schedule	Next Review: December 2024

Table of Contents

Access, Use and Security of Records

INTRODUCTION

The Archdiocese is committed to ensuring that the records needed to support ecclesiastical, canonical and business needs and objectives are available and accessible to relevant staff and other authorised persons in a timely manner. The commitment to availability and access is underpinned by the principles of appropriate openness, collaboration and sharing, and is encouraged in support of delivering significant value and ecclesiastical, canonical and business benefits.

The Archdiocese recognises that the more an information asset is used, the more its value increases.

The Archdiocese manages personal, sensitive and confidential information, and understands the importance of protecting that information while allowing appropriate access. Moreover, records and information of any type and in any format also need to be protected from the risk of unauthorised access, disclosure, alteration, destruction, or accidental or intentional loss.

The purpose of this policy is to provide the mechanisms necessary to facilitate access to and use of information while protecting it against unauthorised access, disclosure, alteration, destruction, or accidental or intentional loss.

This policy is in support of the Archdiocese's information principles, in particular principles 4, 5 and 6 (see appendix 1).

OBJECTIVE

This policy aims to:

- Ensure the provision of records that are reliable, accurate, authentic and inviolate;
- Encourage and support the sharing, collaboration and re-use of records and information;
- Protect records against unauthorised access, disclosure, alteration, destruction, or accidental or intentional loss; and
- Provide a consistent approach to accessing information in a secure environment.

SCOPE

This policy applies to all staff (paid and unpaid), including contractors, consultants and volunteers associated with the Archdiocese and all Archdiocese-owned agencies, organisations and parishes belonging to the Roman Catholic Archbishop of Perth Corporation Sole (the Archdiocese), who create, capture, store and use records in the Archdiocese.

All records, irrespective of medium or format, must be subject to this policy. For example, hardcopy and digital records, including, but not limited to, emails and websites, and records in all business systems, mobile devices, databases, social media and voicemail.

POLICY STATEMENT

Overview

The Archdiocese will take a risk-based approach to managing access to and security of its records. It will develop and implement mechanisms and procedures to manage and control appropriate access to and use and security of its records. This will take into consideration the risks and benefits to ecclesiastical, canonical and business aspects of the Archdiocese and the community as well as ethical considerations and legal requirements.

Records are to be accessible for as long as they are required and disposed of in accordance with the retention and disposal schedule.

Access to and sharing or exchange of information must be achieved in a manner that ensures the security, integrity, privacy and confidentiality of the information.

Access to and sharing or exchange of information and records must not be hindered or denied if the person or organisation has gathered legitimate legal advice to request and receive access.

ACCESS TO AND USE OF RECORDS

Staff Access and Use

Guided by its information principles, and as far as practicable, the Archdiocese will provide an environment of openness to encourage collaboration and the use, re-use and sharing of information. Where legislative and/or ecclesiastical, canonical and business requirements exist, access will be restricted in order to protect personal, sensitive and confidential information. This approach to availability will ensure that information delivers the greatest value to the Archdiocese.

Regardless of format or location, records will be available to all staff to enable them to perform the duties of their role, mindful of the considerations of security, privacy, confidentiality and archival integrity. Under no circumstances will records be accessed or used for other than authorised Archdiocese-related business.

Staff are not permitted to give access to the Archdiocese’s records to unauthorised persons or organisations. All information not generally available to the public should be treated as confidential.

Access to personnel files, regardless of format, is restricted to personnel staff. Individual staff members may request and be granted access to their file.

Public Access and Use

Public access to personal, sensitive and confidential information will be in accordance with the Privacy Amendment (Private Sector) Act 2000 (Cth) and the associated Australian Privacy Principles (APPs), and the Privacy and Confidentiality Policy.

Public access to archives will be in accordance with The Management of Archival Records of the Roman Catholic Archdiocese of Perth, Policy 1.

Public access to other Archdiocese information and records will be by written request to the Chief Executive Officer of the Archdiocese or the Director of the Office of Information Management and Archives of the Archdiocese, stating clearly the nature and purpose of the request.

The Archdiocese will develop and implement guidelines for the management of public access to current information and records, that is, to information it has created and captured that is not held in the Office of Information Management and Archives Services.

Granting external access to records and information will be determined by the information security classification that applies to the information or record and with the approval of the Director of the Office of Information Management and Archives. (See Information Security below.)

Where circumstances deem that it may be appropriate to release restricted or internal records to an external party, this will be conducted under an obligation of confidentiality and with execution of an approved release form. This will occur only where:

- The Archdiocese determines that it has a compelling business reason to release the information or records;
- The release does not breach the Privacy Amendment (Private Sector) Act 2000 (Cth) and the associated Australian Privacy Principles (APPs), and the Privacy and Confidentiality Policy, or other confidentiality obligations; and
- The external party is a trusted party, and there is a high level of confidence that they will adhere to the confidentiality requirements.

Original records must not leave the Archdiocese's control. Only copies of original hardcopy records will be provided to external parties once appropriate approval has been granted. This requirement will apply unless the originals are required by law.

Access to Records via Subpoena or Warrant

Requests for access to records or information via subpoena or legal warrant will be managed by the Director of the Professional Standards Office.

No records or information will be supplied in reply to a subpoena or legal warrant without the approval of Chief Executive Officer of Administration

Any records, or information, that are subject to a request via subpoena or legal warrant must not be destroyed until the Chief Executive Officer of Administration has approved the destruction.

Personal, Sensitive and Confidential Information

In line with its Privacy and Confidentiality Policy, the Archdiocese will develop and implement appropriate mechanisms to ensure the security of personal, sensitive and confidential information. Such an approach aims to protect this information against loss and unauthorised access, use, modification or disclosure.

Information Security

The Archdiocese will develop and implement an information security classification framework to protect and control access to records. The framework will be used to identify the types of records and information that may need to be protected to some degree and the appropriate level of control used to apply that protection.

All records must be categorised according to their level of confidentiality and sensitivity whenever records containing such information are created or received. They must be adequately secured and protected, and kept in accordance with necessary disposal and storage requirements.

Hardcopy and digital documents must be made visually different from each other by the use of protective markings. A physical or digital label must be attached to documents to indicate the assigned information security classification. These include but are not limited to use of:

- Watermarks such as ‘Confidential, Sensitive Information’ or ‘Commercial in Confidence’; or
- Specific text in capitals, bold text.

Hardcopy records used and stored will be secured to avoid possible theft, misuse or inappropriate access.

Hardcopy records must be registered in the records management system.

Hardcopy records may not be removed or moved offsite without the express authorisation of the Director of the Office of Information Management and Archives.

Business systems and applications, including the records management system, will have appropriate security mechanisms to protect digital records and information. This will include, but not be limited to, access and user permissions.

Each staff member who uses the records management system and/or business systems and applications must have an individual login. At no time will staff share their login, access codes or passwords to these systems with anyone.

All staff will ensure that their username and password for all business systems and applications including the records management system are kept secure at all times.

Staff with remote access must apply the appropriate security measures to ensure that the information that they access is not subject to unauthorised access, deletion, destruction or corruption.

A staff member who ceases employment with the Archdiocese must ensure that prior to leaving, all records in their possession or under their control have been captured in the records management system, the relevant business system or the official paper-based system, as appropriate.

SUPPORTING GUIDELINES

Not Applicable

SUPPORTING PROCEDURES

Refer to the Information Management Implementation Plan

RELATED POLICIES

Archives Management Policy
Records Management Policy
Privacy and Confidentiality Policy
Storage and Maintenance of Records Policy

RELEVANT LEGISLATION AND STANDARDS

Director of the Office of Information Management and Archives

RESPONSIBLE OFFICER

Director of the Office of Information Management and Archives
Tel: 6104 3625
Email: archives@perthcatholic.org.au

APPENDIX 1: INFORMATION PRINCIPLES

	Principle	Description
1	**Information is a valued Archdiocesan asset**	The Archdiocese acknowledges the importance of information as a strategic organisation-wide asset. Improving the way it is managed and used should deliver significant value and business benefits.
2	**Information will be managed**	Information assets will be created, captured, stored, managed, protected and optimised in ways that are appropriate to their value. Robust information management will enable appropriate access and use of the assets. Information will be managed according to the information life cycle. Information governance will be applied and compliance with statutory requirements and organisational policy will be ensured.
3	**Information will be trustworthy**	Information created by the Archdiocese will be of sufficient quality to meet the purpose/s for which it is intended. As such, information will be accurate, valid, reliable, relevant and complete. If information is sourced from outside the organisation, all reasonable care will be taken to ensure it is trustworthy. Information will have a single identifiable and accurate source. This will be central to ensuring the trustworthiness of the Archdiocese's information. It will be created once and will be available to be used confidently for different purposes over time.
4	**Information will be shared**	Information will be created, collected, stored and managed with the view to promoting the sharing, collaboration and re-use of these assets. Accurate, reliable, timely and relevant information will be available to share with others who have an appropriate business requirement. The Archdiocese recognises that the more an information asset is used, the more its value increases. As such, the Archdiocese prefers to re-use and build on existing information rather than recreate or re-collect information.
5	**Information will be accessible**	Subject to security and acceptable use policies and protocols, information assets will be accessible in appropriate formats. This availability will ensure that information delivers the greatest value to the Archdiocese.
6	**Information will be protected and preserved**	Information will be protected and preserved. It will be appropriately secured and protected from unauthorised access, use and disclosure.

For enquiries or more information, please contact:

ODHRAN O'BRIEN
Director of the Office of Information Management and Archives
Tel: 6104 3625
Email: archives@perthcatholic.org.au

Location: Office of Information Management and Archives,
193 Harold St, Mt Lawley WA 6050

Postal Address: 40A Mary St, Highgate WA 6003

ARCHDIOCESE OF PERTH