Catholic Archdiocese of Perth

Disaster Management for Records Policy

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

TABLE OF CONTENTS

INTRODUCTION

The Archdiocese is committed to protecting its records and information assets in all formats over time. As such it will develop a disaster management program for these assets that will provide the guidance, resources and training necessary to ensure that the impact of disruptive occurrences and events is mitigated or eliminated.

Central to this commitment will be a disaster management plan that will ensure continued access and useability of records in the event of a disaster or emergency situation affecting the Archdiocese's records, records systems and/or storage areas.

The disaster management program for records and records management systems will fit within the Archdiocese's business continuity framework.

OBJECTIVE

This policy aims to:

- Provide a systematic approach to the management of any disaster or emergency situation that has the potential to damage or destroy the Archdiocese's records;
- Mitigate or eliminate the effect of disasters or emergency situations that may compromise access to and use of records;
- Protect the Archdiocese's records, records management systems and storage facilities in the event of a disaster or emergency situation; and
- Ensure all staff (paid and unpaid) are aware of, and understand the purpose and elements of, disaster management and their roles and responsibilities in any disaster or emergency situation.

SCOPE

This policy applies to all staff (paid and unpaid), including contractors, consultants and volunteers associated with the Archdiocese and all Archdiocesan-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.

In the main, the scope of this policy is focused on hardcopy records. However, the principles and policy positions presented here extend to digital records, which should be accounted for in the information technology disaster recovery plan.

POLICY STATEMENT

The Archdiocese's disaster management program will consist of a policy, a plan and procedures that, collectively and individually, will provide the capability to protect the Archdiocese's records and contribute to business continuity in the case of a disaster or emergency situation.

The approach to disaster management for records will be consistent with the disaster management principles of AS ISO 15489.1:2017, Information and documentation - Records management, Part 1: Concepts and principles.

The Archdiocese will develop and implement a disaster management plan that will address minor and major disasters as well as emergency situations. This plan will address the four phases of disaster management, namely:

- Mitigation;
- Preparedness;
- Response; and
- Recovery.

Any business continuity, risk management or information technology disaster planning will take the records disaster management program into consideration.

The records disaster management plan will form an important part of the Archdiocese's business continuity planning and risk management. It will also complement the information technology disaster recovery plan.

The Archdiocese will commit to testing, maintaining and updating the records disaster management plan, its procedures and processes on a regular basis. The relationships with other disaster management plans will be reviewed and retained.

All staff will be made aware of the records disaster management plan. They will be assisted to understand the purpose and elements of the plan and their roles and responsibilities in the event of a disaster or emergency situation. Training in disaster response and recovery will be provided on a regular basis.

SUPPORTING GUIDELINES
Not Applicable

SUPPORTING PROCEDURES
Business Recovery Plan

RELATED POLICIES
Archives Management Policy
Privacy and Confidentiality Policy
Records Management Policy
Vital Records Policy

RELATED PLANS
Business Continuity Plan
IT Disaster Recovery Plan
Risk Management Plan

RELEVANT LEGISLATION AND STANDARDS
AS ISO 15489.1:2017. Information and documentation - Records management, Part 1: Concepts and principles.

RESPONSIBLE OFFICER
Archivist and Director of Archives Office
Tel: 6104 36 26