Records and Mobile Technologies

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

Introduction 01
Objective 01
Scope 01
Policy Statement 02
Supporting Guidelines 03
Supporting Procedures 03
Related Policies 03
Relevant Legislation and Standards 03
Responsible Officer 03

Records and Mobile Technologies

INTRODUCTION

The Archdiocese recognises that mobile and smart devices can be a method of communication that enables engagement, participation and the sharing and re-use of information in the course of its ecclesiastical, canonical, parish and business activities, functions and operations.

Mobile and smart devices are capable of creating, storing and deleting records. Such records need to be managed as assets of the Archdiocese and subject to sound records management practices.

OBJECTIVE

This policy aims to:

- Provide staff with information and guidance on the appropriate ways in which to manage records created, captured and stored using mobile and smart devices;
- Advise users of mobile and smart devices of their responsibilities with regard to records created, captured and stored;
- Ensure that the content of mobile and smart devices that is related to ecclesiastical, canonical, parish and business activities, functions and operations is managed as a corporate record; and
- Ensure that legislative records management obligations are met.

SCOPE

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

It has particular application to those staff using mobile and smart devices that create, capture and store records related to ecclesiastical, canonical, parish and business activities, functions and operations.

All records created, captured and stored using mobile or smart devices must be subject to this policy.

Mobile and smart devices may include, but are not limited to:

- Internet-enabled and internet-capable devices such as smart phones, tablets, laptops and digital cameras;
- Non-internet portable devices such as handheld sound recorders, portable storage items such as DVDs, memory sticks and iPods, and non-digital photographic equipment.

POLICY STATEMENT

When using mobile or smart devices for ecclesiastical, canonical, parish and business activities, functions and operations, staff must keep accurate and sufficient records documenting these activities. This information needs to be kept in a usable and accessible form for a minimum of seven years.

Staff who have been issued with an Archdiocesan mobile or smart device must transfer, copy and/or synchronise records and information saved in corporate mobile and smart devices into the Archdiocese's records management system and/or approved business system or repository to ensure that records are stored and made accessible. This must be done as soon as possible after their creation or capture on the device.

The Archdiocese will develop, implement and maintain appropriate methods for capturing, storing and managing records created using mobile and smart devices, and the context and content of the records involved.

Records created using mobile or smart devices are subject to the records retention and disposal schedule and must not be destroyed or disposed of without reference to this schedule and/or the Archivist.

Messages such as email, SMSs, instant messages or voicemail received on a mobile or smart device are subject to the same requirements as email messages received on a desktop computer or voicemail on a landline phone.

The Archdiocese will develop and apply a security protocol to protect mobile and smart devices and any information on them.

Staff must apply appropriate security measures in line with the Archdiocese's security protocol to ensure the safety and security of records created and stored on mobile or smart devices. This may include, but not be limited to, for example, a personal identification number, passwords, regular transfer of records to the records management system or approved business system and/or not allowing unauthorised persons access to the device.

Before an entire mobile or smart device is disposed of, all records contained on the device must be captured in the records management system or other approved business system, and any remaining information on the device must be destroyed.

Records management training will include the use of mobile or smart devices.

The Archdiocese will adhere to the Privacy Amendment (Private Sector) Act 2000 (Cth) and the associated Australian Privacy Principles (APPs) when capturing and storing records created using mobile or smart devices.

SUPPORTING GUIDELINES

Refer to the Information Management Implementation Plan

SUPPORTING PROCEDURES

Refer to the Information Management Implementation Plan

RELATED POLICIES

Access, Use and Security Policy
Director of the Office of Information Management and Archives Management Policy
Email Management Policy
Privacy and Confidentiality Policy
Records Management Policy

RELEVANT LEGISLATION AND STANDARDS

Privacy Amendment (Private Sector) Act 2000 (Cth) and the associated Australian Privacy Principles (APPs)

RESPONSIBLE OFFICER

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

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