Data Governance

Table of Contents

Data Governance

Purpose

The purpose of this policy is to

- Provide an overarching approach and common understanding to ensure the Archdiocese's data is appropriately managed and governed;

- Define the roles and responsibilities for different data creation and usage types, cases and/or situations, and to establish clear lines of accountability;

- Develop best practices for effective data management and protection;

- Ensure that the Archdiocese complies with applicable laws, regulations, exchange and standards; and

- Ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, exchanging, reporting, managing and storing of data.

Scope

This policy applies to:

- Employees and Volunteers; (referred to in this Policy as Staff/Staff Members)

- All Archdiocese-owned agencies, offices and organisations belonging to the Roman Catholic Archbishop of Perth Corporation Sole, who create, capture, store and use records and data in the Archdiocese.

- and Consultants and Contractors

Subject Matter

The Archdiocese's corporate data is valued as a strategic asset, essential to support ongoing operations and functions, and provide valuable evidence of ecclesiastical, canonical and business activities over time.

The purpose of this policy is to help ensure the governance, classification and protection of data from unauthorised access, damage, alteration or disclosure while preserving the ability of authorised users to access and use institutional data for appropriate purposes.

Policy

The ownership and custody of the Archdiocese's data assets, resides with the Archdiocese irrespective of whether it was received or created by Archdiocese employees, contractors, consultants, volunteers and organisations performing work on behalf of the Archdiocese.

Roles and Responsibilities

- The Archbishop, as owner, is accountable for the overall appropriateness and compliance of the Archdiocese's data to the requirements of the

    - National Catholic Safeguarding Standards and

    - The Archdiocese's Information Governance Strategy.

- The Archbishop delegates responsibility for the Archdiocese's data governance program to the Archivist, as the custodian of data. Archives and Information Governance Office (AIGO) are responsible for the ongoing effectiveness of the data management program,

- All Executives and Managers are to ensure the implementation of this policy. It is the responsibility of each Executive and Manager to champion the value of data governance to their business areas and to encourage adherence to and support for the Archdiocese's data governance program.

- All Archdiocese employees are responsible for ensuring that data created as a result of their official roles, regardless of type, format or media, is managed in accordance with the Archdiocese's Information Governance Strategy.

- All owners of business systems that store data must understand their responsibilities and obligations related to their system/s and associated business processes that they manage and/or use. As such, they must adhere to the Archdiocese's Information Governance Strategy.

Data Stewardship

Reliable data stewardship is essential to ensure that data is collected, maintained and used appropriately. Good custodianship of data provides accountability for datasets and gives the user confidence in the level of integrity, timelines, precision and completeness of data.

Data Steward

Each business area requires a Data Steward who are subject matter experts in the related functional area and who has knowledge of the business data and processes within it.

Their responsibilities include:

- Working with the Information Technology Services on data system design that covers data creation, classification, migration, access management, disaster management, migration and retention and disposal;

- Implementing and maintain data quality requirements and business rules for assigned data sets;

- Identifying, managing, mitigating and resolving (where applicable) data issues, risks and errors; and

- Championing and educating their functional area on the use and application for the data management framework and supporting documents.

Data Custodian

AIGO fulfils the role of Data Custodians and are responsible for the security and availability of the Archdiocese's data. Their role is to oversee systems used to collect, manage and provide access to data.

Their responsibilities are:

- Maintain physical and system security including server physical security and user access security as determined by the Data Steward;
- Ensure adequate system backups are completed and disaster preparedness and recovery plans exist; and
- Ensure adequate system availability and performance.

Data Creators

Refers to Archdiocesan employees who collect, create and/or deposit data into data collections held in business systems. Their role is to

- Accurately capture data in line with their business responsibilities and relevant legislative, policy and standard requirements;
- Implement appropriate procedures to uphold the quality and integrity of the data they create and access; and
- Seek advice from Data Stewards and Data Custodians when modifications are required to data collection requirements in business systems.

Data Management Principles

The Archdiocese's corporate data must be:

- Managed as a strategic asset through clear processes, procedures, standards and guidelines;
- Actively managed throughout the data lifecycle, from collection to disposal, and stored in approved and appropriate information systems; and be
- Secure and reliable, while also accessible for authorised use in accordance with clear and transparent control frameworks.
- Every data source must have a defined Data Custodian and Data Steward, who act in a business leadership role and a subject matter expert role;
- Data should only be collected and readily available for use, for a specific and documented purposes, in a simple, user centric approach that supports and enables data value to realised;
- Data capture, validation and processing should be automated, wherever possible;
- Unnecessary duplication of Archdiocese data is to be avoided;
- Data is managed through approved, managed structures and models that provide context and a best practice approach that enables active data lifecycle management; and
- Data must be protected from unauthorised access and modification.

BREACH OF POLICY

Failure to comply with this Policy by a staff member may be considered a breach of the Code of Conduct and may result in disciplinary action.

LEGISLATION

Corporations Act 2001 (Cth)
Privacy Act 1988 (Cth)

AUTHORITY

National Catholic Safeguarding Standards
Serving the Church in the Digital Age: The Archdiocese of Perth's Information Governance Strategy

ASSOCIATED DOCUMENTS

Creation, Capture and Control Policy
Approved Information Governance Policy suite.

Version	Date Issued	Approved By	Amendments Undertaken
1.0	16.05.23		Align visual style with other documents, minor text changes, Text changes, removal and adding of pages

For enquiries or more information, please contact:

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

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

Postal Address: 40A Mary St, Highgate WA 6003

Before referencing this document, please ensure you
have the latest version from the Archdiocesan Intranet.
Printing of this document is not recommended.