Melbourne Archdiocese
Catholic Schools

Data Policy

1. Introduction

Melbourne Archdiocese Catholic Schools (**MACS**) is a company limited by guarantee established in 2021 by the Archbishop of the Catholic Archdiocese of Melbourne to assume the governance and operation of MACS schools across the Archdiocese of Melbourne. MACS subsequently established Melbourne Archdiocese Catholic Specialist Schools Ltd (**MACSS**) to provide educational services to children with special needs and Melbourne Archdiocese Catholic Schools Early Years Education (MACSEYE) to provide early years care and education services.

The Statement of Mission in the MACS Constitution, and the constitutions of its subsidiaries, MACSS and MACSEYE, sets out the Archbishop's expectations of Catholic schooling in the Archdiocese and provides an important context and grounding for the company and the direction which the MACS Board must always observe in the pursuit of the company's objects.

The Board must ensure that all policies and procedures concerning the operations of MACS, and its subsidiaries are consistent with the Statement of Mission and company objects, as well as any directions issued by the Archbishop from time to time.

2. Purpose

This policy provides the foundation for data management and governance at Melbourne Archdiocese Catholic Schools Ltd (MACS) with a focus on maintaining solid technical and organisational infrastructure, standards and processes that enable the effective, consistent and secure collection, analysis and sharing of data.

3. Scope

This policy applies to all data within MACS offices and MACS schools, including that used by MACS employees, contractors, consultants, volunteers, and other users (collectively **Staff**) as well as students and parents/carers (both current and prospective). It is applicable to data assets in any form including electronic, printed, written and spoken and includes backups and archived data as well as live data.

4. Principles

The following principles underpin the policy directives:

- Data is a strategic asset

  Data must be viewed as a strategic asset that is used to support decision making at all levels (individual, class, cohort, school, regionally and globally) and which enables insights into how improved outcomes for students and school communities can be achieved. This is in alignment with the *MACS2030 Strategy* and the vision of the MACS Digital Ambition principle of being 'data Informed'.

- Data must be accessible

  Data must be accessible based on role-based needs to be used in ways that add value within and across MACS offices and MACS schools. Staff must be encouraged to use data to support prudent decision making at all levels and therefore have controlled, yet efficient access to data.

- Data must be trusted and reliable

  The quality of data within MACS must be optimised in order to foster trust in available data and its use in accurate decision making at all levels. Completeness, consistency, reliability, timeliness, uniqueness, validity and accuracy of data must be ensured.

There is a risk of incorrect decisions and reputational impact if data is not interpreted and applied consistently. Data must be accurate and consistently defined so that valid interpretation and well-informed decision making are assured.

- Organisational risk related to data must be minimised

  Improper use and disclosure of data is a business risk with legal, financial and reputational implications. Such risk must be minimised by ensuring privacy and security of data.

5. Policy

5.1. Application and system selection

When proposing, scoping, designing and/or developing systems or applications that will store or handle data pertaining to MACS, the principles and requirements included in this policy must be met.

5.2. Data governance

A defined data governance approach must exist at MACS offices and MACS schools to ensure holistic control of data assets so that MACS can get the most value from data. Such control should also extend to guiding technical implementation by providing standards, guidelines, taxonomies and conventions on data-related implementations.

The governance approach must be executed by a formally defined governing body comprising of cross-functional representatives from various business units including but not limited to IT. The group must oversee all data management practices and establish and enforce data governance policies and standards.

Domain experts who have expertise on particular data sets must be identified. These experts must be given stewardship of data and accountable for the ongoing quality of data so that it can be relied upon for decision making at all levels.

5.3. Data centralisation

Data used for strategic decision making must be available centrally and accessible using a standard set of tools removing the need to access data from multiple sources using multiple tools.

Supporting systems must be in place to consolidate fragmented data repositories and make data discoverable at one location.

Non-centralised data should be used only on a tactical basis in cases where business continuity is immediately affected by the time taken to centralise the data. Such usage must be based on approval by a governing body and a positive privacy impact assessment. A clear plan must be present for each such non-centralised usage to be subsequently ported to centralised usage.

5.4. Data quality

Accuracy, completeness, consistency, reliability, timeliness, uniqueness and validity of data must be ensured using data quality assurance processes and systems. Ongoing data quality should be ensured by continuous monitoring of data quality metrics.

High quality, reliable data must be used for decision making, reducing the risk of incorrect decisions

5.5. Enterprise Data Model

An integrated view of the data produced and consumed across MACS must be available as a central enterprise data model. This model must define data using business terms and have tools that present a data catalogue facilitating data item discovery by non-technical users.

The enterprise data model must provide a central, unbiased interpretation of data, ensuring that any data used for decision making is unambiguous and minimises the risk of poor decision-making.

Metadata must be stored about each data item in the enterprise data model. Metadata must be used to summarize basic information about a data item such as domain, source, owner and

sensitivity. The additional definition given by metadata will ensure that data users use the correct data. Metadata will also ensure that users can easily decide on the data items they need to use.

5.6. Master Data Management (MDM)

Core business entities within MACS, such as schools, staff, students, parents and subjects should be identified as master data. Each core entity may originate from multiple sources and should be de-duplicated, reconciled and enriched to become a consistent, reliable source.

Each master data entity's structure should be defined, including all its attributes. Validation metadata should be defined for each attribute to facilitate consistent and accurate data through validation.

Once created, master data should be made available as a view of trusted business data that can promote accurate reporting, reduce data errors, remove redundancy, improve efficiency and help users make more accurate, well-informed decisions.

5.7. Data access

Relevant users must be given convenient access to data. However, data must not be exposed in an uncontrolled manner. Role based access control must be used to control access to data. Such access must be reviewed periodically.

Direct access to curated data should be allowed where there are suitable tools that enable a user to perform read-only consumption of the data, and the user is sufficiently trained in using the tools. In all other situations, data must be accessed through abstractions and visualisations that present the data in a format that is immediately usable to an end user.

Data access must not be granted by default. A defined process must exist for a user to request access to a data set and have that request reviewed and approved or rejected.

Automated flow of data between systems must be defined and controlled. The definition must adhere to a standard template and be approved by a technical group with approval authority.

5.8. Privacy and data security

Data must be gathered only for legitimate uses which are aligned with the MACS mission and add value to MACS.

Security must be ensured for data in transit and in storage as guided by the Cyber Security Policy and the Privacy Policy.

Each data item must be classified by data sensitivity in accordance with the Data Classification Guidelines.

Data must be handled, retained and disposed based on classification in accordance with the Data Handling Guidelines and in alignment with Information and Records Management Procedure – Retention and Disposal.

Data loss prevention methods must be applied across on-premises systems, cloud-based locations, and endpoint devices to prevent unsafe or inappropriate sharing or transfer of data.

6. Definitions

Definitions of standard terms used in this Policy can be found in the Glossary of Terms.

Curated Data

Data that has been collected, integrated and organised to enable analysis.

Data

A subset of information in an electronic format that allows it to be retrieved or transmitted.

Data Catalogue
An inventory of all the data that an organization collects and processes.

Data Governance
Overall management of the availability, usability, integrity, and security of the data employed in an enterprise.

Domain Expert
An expert on a particular data set who understand business processes, best practices, regulatory requirements, and common challenges about that data better than anyone else.

Metadata
Data that describes various facets of another data item and thereby improves its usability across its lifecycle.

7. Related policies and documents

Supporting documents

Data Classification Guidelines
Data Handling Guidelines

Related MACS policies and documents

Cyber Security Policy
Information and Records Management Policy – MACS office
Information and Records Management Procedure - Create Capture and Control
Information and Records Management Procedure - Storage and Access
Information and Records Management Procedure - Retention and Disposal
Privacy Policy
Risk Management Policy
Child Safety and Wellbeing Recordkeeping Procedures

8. Legislation and standards

Privacy Act 1988 (Cth.)

9. Policy information

Responsible director	Director, Finance, Infrastructure and Digital
Policy owner	Chief Technology and Transformation Officer
Approving authority	Executive Director
Assigned board committee	
Approval date	5 February 2025
Risk Rating	High
Review by	February 2029
Publication	MACS office Intranet, CEVN

POLICY DATABASE INFORMATION	
Assigned framework	Governance
Supporting documents	See list of supporting documents and related policies above
Superseded documents	CEM Data Policy
New policy	New