Privacy Policy

Preamble

Marists belong to one of the rich spiritual families in the Church. Their personal faith, manner of sharing in the mission of the Gospel and means of forming Christian community are all shaped by the spiritual way introduced into the life of the Church by Marcellin Champagnat. Marist Brothers and lay people share in our mission in education, social justice and supporting the poor and marginalised.

The Trustees of the Marist Brothers have the ultimate canonical and civil authority of all Australian assets and activities of Marist Brothers Star of the Sea Province. The Australian activities of the Marist Brothers Star of the Sea Province are conducted directly through the Trustees with the exception of Marist Youth Care, Australian Marist Solidarity, Marist School Australia Limited and the Marist Association of St Marcellin Champagnat Limited which are all separately incorporated entities.

Marist Schools Australia Limited (MSA Ltd) is a public not-for-profit company limited by guarantee and registered with the Australian Charities and Not-For-Profit Commission. Its purpose is to advance education and religion, specifically to make Jesus Christ known and loved and to ensure quality Catholic education in the Marist tradition through its schools.

The Marist Association of St Marcellin Champagnat Limited (MASMC Ltd) is a not-for-profit company limited by guarantee which was formed by the Trustees of the Marist Brothers to provide governance as well as spiritual leadership and formation for those engaged in the apostolic works, activities and operations of the Marists in Australia. MASMC Ltd is the sole member of MSA Ltd.

Definitions

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether the information or opinion is true or not, or whether it is recorded in a material form or not.

Sensitive information is a subset of personal information, which is given a higher level of protection under the Privacy Act. It includes, amongst other things, health information, criminal record, religious beliefs or affiliations.

Policy Statement

The Trustees of the Marist Brothers, and related entities, are committed to managing personal information in accordance with the Australian Privacy Principles ("**APPs**") under the *Privacy Act 1988 (Cth)* ("**Privacy Act**") and in accordance with other applicable privacy laws.

All staff employed by the Trustees of the Marist Brothers, and related entities, have a responsibility to make themselves familiar with the requirements of their rights and responsibilities to ensure their compliance with the Privacy Act 1988 *(Cth)* and the contents of this policy. Staff will be informed of changes that may occur from time to time and they must ensure they maintain a current understanding of these requirements.

This policy complies with the Privacy Act and the APPs. It is based on a principle of respect for the personal information of staff and others that is provided to the employer for the primary purpose for which it was lawfully collected.

Purpose

This policy sets out the practices with regards to the collection, use and storage of personal and sensitive information of staff and those engaged by the employer and the obligations on staff when handling such information of others within their roles.

Scope

This policy applies to all staff (employed or engaged by the employer and is inclusive of Brothers, other religious, clergy and contractors and sub-contractors) of the Trustees of the Marist Brothers ("**Marist Brothers**"), Marist Schools Australia Limited ("**MSA Ltd**") and the Marist Association of St Marcellin Champagnat Limited ("**MASMC Ltd**") (collectively referred to in this Policy as the "**employer**"). This policy is not intended to cover staff in Colleges as they are required to comply with their own College's policy.

Application

1. Collection, use and storage of personal and sensitive information

1.1 Information is generally collected by way of forms which are filled out either by the individual or their representative online, in face-to-face meetings, interviews and telephone calls.

1.2 In some circumstances, a third party may provide personal information, such as a reference about an applicant for a position.

1.3 Staff and others are free to decline requests from the employer for personal or sensitive information, but in some cases that may result in the employer not being able to assess the suitability of a person for employment.

1.4 Personal information about other individuals may be requested of staff (for example, spouse, dependants or other family members. If so, the staff member has the obligation to inform those individuals about the disclosure and the Privacy Policy.

1.5 It is not practical in the employment relationship for staff, or potential staff, to provide their personal information anonymously.

1.6 Personal information that is collected from staff and others will only be used for a lawful reason such as when it is our legal duty, if we have your consent and when it's in our legitimate interest to do so.

1.7 Reasons for collecting personal information include:

1.7.1. For purposes relating to the employment of staff, contractors and sub-contractors and others, including recruitment purposes such as pre-employment screening, contacting referees, processing applications, and assessment for suitability for future positions.

1.7.2 For governance and compliance purposes including managing any quality, conduct or risk management issues including conflict of interest.

1.7.3 Meeting regulatory obligations, and where required to or authorised by legislation or industry code, direction or standard to do so.

1.7.4 Other purposes related to our business.

1.8 The employer may also use non-personal, de-identified and aggregated information for several purposes related to improving our services. Any output is anonymised or aggregated so that no personal information or information relating is reasonably identifiable.

1.9 The employer may disclose staff or other personal information to others for legitimate purposes such as to another Church agency, government departments, medical practitioners, people providing services to the employer, where required by law or court order and anyone that is authorised by the staff member. No overseas disclosure of personal information will occur unless authorised by the staff member.

1.10 Recipients of personal information held by the employer (as per 1.9) will be provided will be required to adhere to and have similar privacy policies.

1.11 Staff are required to respect the confidentiality of the information and privacy of colleagues and others that they may handle or become aware of in the course of their work.

1.12 Staff must not misuse, interfere with, access without authorisation, modify or disclose any personal information held by the employer. Any breach of this direction will be taken seriously and may result in disciplinary action up to and including termination.

1.13 All personal information is held securely in electronic files with restricted access. Hard copy information must be held under lock and key and staff are to ensure that paper documents, keys and passwords are securely managed.

1.14 The employer may be obligated by law to report data and other breaches of the Privacy Act to the relevant Privacy Commission regardless of whether the breach was deliberate or accidental. The employer will need to act urgently and directly to rectify any breach by advising individuals who have had their personal information misused or incorrectly disclosed, enacting remedies and altering security or processes to reduce or eliminate the risk of any further breach.

1.15 The employer will endeavour to ensure that the personal information held is accurate, complete, and up to date, and where using or disclosing it, relevant for the purpose of the use or disclosure.

1.16 A staff member or other person engaged by the employer may seek to update the personal information held about them by contacting the Payroll Officer or Human Resources Officer. This request should be in writing as a statement with the information that you believe is inaccurate, out-of- date, incomplete, irrelevant or misleading.

1.17 Any personal information that we hold about staff and others can be accessed by that person, after proper identification, according to certain conditions under the Privacy Act and the Fair Work Act. Request for access is to be made in writing to the Human Resources Officer.

1.18 According to the legislation access to some personal information held by the employer may not be possible, particularly where it may relate to the privacy of another person. If this occurs the requesting person will be provided the reasons for denying access in writing.

1.19 Personal information belonging to job applicants who are not recruited will either be destroyed or retained with the permission of that person for possible future employment consideration.

1.20 Where personal information held by the employer is no longer required for a purpose for under the Privacy Act, all reasonable steps will be taken to destroy or de-identify that information, unless it would be unlawful to do so.

1.21 Some examples of the personal information that is collected from staff and others engaged by the employer, which may include sensitive information, includes:

1.21.1 Candidate information (such as a resume) submitted and obtained from the candidate and other sources in connection with applications for employment.

1.21.2 Work performance information (such as evaluations or reviews or work performance).

1.21.3 Information pertaining to incidents in the workplace.

1.21.4 Statement of employment, banking details, tax file number

1.21.5 Information submitted and obtained in relation to absences from work due to leave, illness or other causes.

1.21.6 Education transcripts and certificates.

1.21.7 Test results (such as psychological evaluations).

1.21.8 Working Visa information.

1.21.9 Information about next of kin

Breach of Policy

A breach of this policy may result in disciplinary action, including termination of employment. It may also result in notification to an external agency such as the Privacy Commission within the relevant jurisdiction or the Office of the Australian Information Commissioner.

Complaints about the handling of personal information

Any complaints, questions or concerns ('**complaint**') about this Privacy Policy or about the way in which personal information has been handled may be raised with your Ministry Leader or Manager.

The Ministry Leader or Manager will first consider whether there are simple or immediate steps which can be taken to resolve the complaint.

If your complaint requires more detailed consideration or investigation, we will acknowledge receipt of your complaint within a week and endeavour to complete our investigation into your complaint promptly. We may ask you to provide further information about your complaint and the outcome you are seeking. We will then typically gather relevant facts, locate and review relevant documents and speak with individuals involved.

In most cases, we will investigate and respond to a complaint within 30 days of receipt of the complaint. If the matter is more complex or our investigation may take longer, and we will let you know.

If you are not satisfied with our response to your complaint, or you consider that the employer may have breached the Australian Privacy Principles or the Privacy Act, a complaint may be made to the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner can be contacted by telephone on 1300 363 992 or by using the contact details on the website *www.oaic.gov.au*

Monitoring and Reporting

This policy will be monitored, any breaches managed, and the operation of the policy reviewed for improvement.

Related Policies and Documents

- Code of Conduct
- Acceptable Use of Electronic Communication Systems and Devices

Further Information

Further information or assistance about anything contained in this policy can be sought from your Ministry Leader or Manager.

The Privacy Commission in each jurisdiction provides resources and receives and responds to privacy breaches and complaints covered by their legislation.

Confidential support for work-related or personal concerns is provided for all staff through the Employee Assistance Program. Access EAP can be contacted on 1800 818 728.

Policy Owner:	Province Director of Finance and Business MSA Head of Business
Version Number:	1.0
Publication Date:	26 May 2023
Approved By:	Vice-Provincial, Marist Brothers MSA National Director, Marist Association Executive Officer
Review Date:	26 May 2025