Privacy Policy

This Policy instrument was approved by the Senior Manager Risk and Governance on 20 December 2024

Index

Scope

Marist180 as an agency recognises the importance of protecting the Privacy and the rights of individuals in relation to their Personal and Sensitive Information. This Privacy Policy applies to all Staff, Clients, donors and prospective doner information from third parties, and users and subscribers of the Marist180 website.

Marist180 complies with the *Privacy Act 1988 (Cth)* and *Children and Young Persons (Care and Protection) Act 1998 (NSW),* and the *National Catholic Safeguarding Standards.*

Purpose

This Policy indicates how Marist180 uses, collects, stores, discloses and handles Personal and Sensitive Information. Marist180 is committed to openness and transparency and ensuring that the reasons we require Personal and Sensitive Information about Staff and Clients are clear and in accordance with the current legal requirements.

Policy

Marist180 is committed to promoting a culture that respects the Privacy rights of all Staff and Clients, ensuring that they have a right to Privacy and Confidentiality.

Marist180 is committed to accountability and transparency in order to comply with the following:

1. Children and Young Persons (Care and Protection) Act 1998 (NSW) Chapter 16A
2. Child Protection Act 1999 (QLD) Chapter 5A
3. Children and Young People Act 2008 (ACT) Part 25
4. Privacy Act 1988 (Cth)
5. The Australian Privacy Principles (APP).
6. Health Records and Information Privacy Act 2002 (NSW)
7. Health Records (Privacy and Access) Act 1997 (ACT)

Marist180 ensures the Privacy of Staff and Clients is upheld by:

- Provision of clear and transparent guidance and effective processes regarding the collection, handling and protection of Personal and Sensitive Information concerning individuals and Marist180 Confidential business and operating information.
- Recording and obtaining only necessary information with regard to service provision for Clients, to assist Clients or to promote welfare of the Clients
- Obtaining only necessary information with regard to employment files for Staff
- Storing all records and files related to Clients securely and systematically
- Advising Clients of Marist180's legal responsibilities regarding Personal Information and clearly defining the limits to Confidentiality where this applies
- Adhering to ***Chapter 16A of the Children's Care and Protection Act***, relating to the exchange and collection of information concerning children
- Providing a process of access to information and files that recognises the rights of individuals to view information that is recorded about them and to correct any information that may be out of date or no longer relevant
- Not releasing Personal, Sensitive or Confidential business or operating information without proper authorisation or consent and will never be sold or used for personal gain
- Only seeking to obtain information in an appropriate and Confidential manner

A breach of this Policy by any Marist180 personnel may result in disciplinary action, up to and including termination of employment or other appropriate sanctions.

Collection of Information

Marist180 may collect any information about Staff, Clients, other individuals or any specified body (with consent) including any recorded visual or audio material, such as, but not limited to:

- Personally identifying information (Name, Address, Date of birth etc)
- Sensitive Information (Gender, race, health record, criminal record etc)
- Biometric information (Behavioural characteristics etc)
- Demographic information (Employment, income, ethnicity, education etc)
- Information relating to the applicants assessment criteria
- Information relating to the National Criminal Check and Working with Children check

Consent must always be obtained by Marist180 in order to collect your Personal Information. *[Use Authority to Obtain and Release Information Form, Media Consent Form]* Consent does not have to be in writing, but best practice is to keep a record of a person's consent in their specified files related to Clients. Voice recording may also be used when consent is sought over the phone. It is important that Staff convey to Clients the reason for collecting their Personal Information and to ensure full capability of understanding why they are giving information.

Exchange of Information

The ***Children and Young Persons (Care and Protection) Act 1998*** elevates child protection issues over privacy in NSW in certain circumstances. Under Section 16A information may be exchanged between individuals working with children and young people when:

- The exchange of information is related to the safety, welfare or wellbeing of a child or young person.
- The information is relevant to the purpose for which it is being shared
- The information is shared only with those who "need to know" in order to promote the wellbeing of the child or young person.
- Information about the child's or young person's parent/carer is shared only where this is relevant to the safety, welfare or wellbeing of the child or young person

Marist180 will ensure that, unless ***Chapter 16A of the Children and Young Person's Care and Protection Act*** applies, the correct form of consent will be obtained. Clients are only able to give their consent if they are over the age of 16, if the child is under the age of 16 and no parental guardian is available, the consent of that child will be considered as legally acceptable.

Different regulations apply to the release of information in relation to clients in other States. If a request of information relating to a client in another State is made, it is important that the individual requirements of that State are adhered to. By way of example, in the ACT sensitive information may not be shared unless under very specific conditions. Please ensure you refer to the *Release of Information Procedure* for specific details.

Sensitive Information

Marist180 may sometimes be required to collect Sensitive Information from individuals to provide particular assistance. Such assistance could include facilitating arrangements with, or on behalf of, individuals for financial assistance, accommodation, community engagement, obtaining legal advice and medical and/or mental health assistance.

Marist180 will limit the collection, storage, use and disclosure of Sensitive Information to instances where the information is:

- directly relevant to the purpose for collection,
- reasonably necessary to carry out its functions or activities,
- required by law.

Marist180 will explain the purpose for which Sensitive Information will be used, provide individuals the opportunity to discuss any concerns they may have, and record in Marist180 Authority to Obtain and Release Information Form.

National Criminal History Check

Marist180 may collect information and supply it to third parties as part of conducting a National Criminal History Check as a necessary part of carrying out its functions and activities. Currently, Marist 180 uses Referroo as a third party to conduct criminal history checks. Staff are encouraged to review their privacy policy for any additional information about this process.

Unsolicited Personal Information

If Staff receive any unsolicited Personal Information, the relevant recipient must determine whether the information is reasonably necessary for, or directly related to, one of Marist180's functions.

Unsolicited personal information is any information received by Marist180 where no steps have been taken to collect the information. Examples of unsolicited Personal Information include misdirected emails, correspondence not requested, unrequested documents that contains names and addresses or promotional material containing personal information.

If the Staff member determines that Marist180 is not reasonably necessary for, or directly related to, one of Marist180's functions, the Staff member must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

Where unsolicited information is received it must be destroyed or deidentified within a reasonable period.

When Personal Information requested is not provided

Individuals can decline to provide Personal Information. However, if the Personal Information requested is not provided Marist180 may not be able to:

- provide the requested services (or information about those services), either to the same standard or at all
- engage an individual as a volunteer, member, employee or contractor or volunteer
- employ or enter into a contract with an individual
- meet funding, professional and legal obligations
- respond to a complaint
- tailor the content of our websites which might impact the experience of our websites.

Storage, Retention and Security of Information

This Policy aims to ensure Confidential Information that is recorded and stored in files across the agency is held with the rights and Privacy of those individuals in mind.

Marist180 takes reasonable steps to ensure all Personal Information is protected from misuse, loss and unauthorised access, modification and disclosure. We may hold information in either electronic or hard copy form which are stored securely for your protection. ***[See Information Security Policy]***

Marist180 will hold your Personal files for a minimum of seven (7) years in order to comply with the current laws and legislations. Files relating to Aboriginal and Torres Strait Islander Clients will be kept indefinitely as per legislative requirements.

Marist180 may also obtain Personal and Sensitive Information about you after you have completed the program of which you were involved in, in order to assess your situation after your time with Marist180. Some Personal Information is destroyed or de-identified after service provision ceases.

When holding information, Marist180 will not adopt a client's Government Related Identifier to identify any individual in its own records. A Government Related Identifier is any information that is used to identify an individual that is provided by a State or Territory government or agency. This includes Medicare numbers, Centrelink Reference numbers, drivers licences or passport numbers. "Adopting" a Government Related Identifier includes organising a client's personal information with reference to that identifier; for instance, using a Young Person's Medicare number as the basis for our own identification system.

Marist180 will electronically store all information relating to Police Checks (application forms, informed consent statements, identity documents, and Police Check results) in a structured electronic directory on the Marist180 server, with records stored by calendar month and an electronic summary (spreadsheet) of all Police Check documents stored.

Use of Information

Marist180 and its related agencies comply with ***Privacy Act 1988 (Cth)*** when collecting and managing Personal and Sensitive Information. The information we collect from you or from an authorised third party will be held by the entity that collects it. It will be used to deliver services and to meet our legal responsibilities. We may also use your information within the agency as a whole, to plan, coordinate and improve the way we provide services.

Marist180 collects your Personal Information in order to perform our business activities and functions and to provide the best possible quality of work in your specific circumstance. Marist180 may use your Personal Information to:

- To advise about, assess eligibility for, and provide, Marist180 services and to meet funding, professional and legal obligations in the provision of services
- Send communication requested by you
- Update our records and keep your contact and Personal details up to date
- Comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator or in co-operation with any government authority
- to effectively undertake its business activities and functions, including:
    - keeping individual's records and contact details up-to-date

- complying with workplace relations, human resources, and workplace health and safety obligations including workplace claims management systems
- processing and responding to complaints
- marketing and communications
- responding to media requests (dealt with in accordance with the Media and Public Statement Policy, which also outlines consent requirements) organisational planning
- service development and quality control
- research, monitoring, advocacy and evaluation
- publishing de-identified Personal Information in submissions and reports
- meeting funding, audit and regulatory reporting requirements through the provision of de-identified Personal Information
- complying with any law or court/tribunal orders
- complying with regulatory authorities and government requirements
- fundraising purposes.
- accreditation purposes
- family finding services

Information relating to Clients may be used during external audits, primarily to facilitate welfare and safety of such and to ensure Protection of Clients.

Disclosure of Personal Information

Marist180 may disclose your Personal or Sensitive Information in accordance with *The Freedom of Information Act 1982 (Cth), Children's Guardian Act 2019 (NSW) , Privacy Act 1988 (Cth) and Children and Young Persons (Care and Protection) Act 1998 (NSW) and the National Catholic Safeguarding Standards.* to:

- Government bodies related to the delivery of or more services provided by Marist180.
- Staff, related bodies corporate, contractors or service providers for the purpose of operation and to provide you with the best possible outcome for your situation
- Suppliers or third parties which we have commercial relationships or contractual agreements with for business and purposes relating to your specified case
- Any organisation for any authorised purpose with your consent

We may combine or share any information that we collect from you with information collected by any of our related bodies corporate in order to achieve the best results for you.

Clients are able to OPT out of information disclosure to third parties or external audits by selecting the OPT out option on the Consent Form or via email notice to communications@m180.org.au

Marist180 is legally able to obtain and disclosure information without consent if it directly relates to the safety, welfare and wellbeing of Clients. Such information is considered as, but not limited to:

- Where there is a reasonable suspicion of or potential for the abuse of children, elderly persons, or vulnerable adults
- Where you present a serious danger to yourself or others

- When we are subpoenaed by a Court due to Civil or Criminal litigation, or required by County, State or Federal laws

Marist180 will disclose your Personal and Sensitive Information or Criminal Check Outcome to third party bodies which are administrators of funding for Marist180 programs and services. The below relationships are governed via contractual deeds/agreements to perform quarterly consultation meetings and monthly reporting for all prospective Staff and Clients. Marist180 may disclose your Personal and Sensitive Information to the below third parties which can be contacted on the details provided below:

Department of Communities and Justice
Phone: 1800 000 164
Privacy@facs.nsw.gov.au

National Indigenous Australian Agency
Phone: 1800 079 098
PO Box 2191

Department of Home Affairs
Phone: 13 18 81
101 George Street, Parramatta NSW

Marist180 will not disclose your Personal or Sensitive Information to any offshore record keeping bodies.

Access and Correction of Information

You may request access to any Personal or Sensitive Information we hold about you at any time by contacting us (see contact details below). Where we hold information that you are entitled to access, we will try to provide you with suitable means of accessing it (via email, mail). Marist180 may grant access to your Personal Information to a Third Party only if your consent has been obtained or as required by law.

There may be instances where we cannot grant you access to the Personal Information we hold. This may occur if granting access to this information would:

- Interfere with the Privacy of others;
- Result in a breach of confidentiality;
- Pose a serious risk to a person's safety; and/or
- Likely be prejudice during the preparation for or conduct of proceedings before a Court or Tribunal.

If the above does occur, we will provide you with a reason as to the refusal.

Marist180 is required to provide applicants access to their police check results upon request. If a dispute does occur regarding the results of the police check, the responsible officer will take you through the requirements of appealing the police check results. Marist180 will obtain the required information and documents from you to support your claim of a dispute. Your dispute will be lodged into the National Database to begin investigation after which Marist180 will be informed of the successful or unsuccessful dispute outcome. Marist180 will advise you of your Criminal Check Dispute Outcome.

If you believe that the information we hold about you is incorrect, incomplete or not up to date, you may request to amend it by contacting us via phone, email or post (details below).

Document Security

Staff are required to ensure that all documents relating to the Agency and Clients are secure at all times. This includes ensuring that no printed material is left unattended at printer locations or elsewhere. If unattended material is located, Staff must dispose of these using the designated security bins.

Contact Details

Contact Us

Where you believe that there has been a breach of your privacy, please use the contact details below to contact our Privacy Officer or follow this link to submit your concern online.

We will treat your request or complaint confidentially. Marist180 will aim to resolve complaints in a timely, satisfactory, fair and transparent manner in accordance with Marist180's Feedback and Complaints Management Policy.

Organisation Name: Marist180

Attention to: Privacy Officer

Mailing Address: PO Box 451, Blacktown NSW 2148

Phone Number: 02 9672 9200

Email: privacy@m180.org.au

Where individuals are not satisfied with the results of the complaint, depending on the nature of the complaint, they or their nominated person can make a complaint to:

- the Office of the Australian Information Commissioner in writing to GPO Box 5218, Sydney NSW 2001, by fax (+61 2 9284 9666), or by email to enquiries@oaic.gov.au
- the NSW Privacy Commissioner (for concerns related to NSW health records)
- the Privacy Commissioner by telephone on 1300 363 992 (enquiries only)
- the NSW Ombudsman on 9286 1000 or www.ombo.nsw.gov.au.
- ACT Privacy Commissioner (for concerns related to NSW health records)

Legislation

Australian Crime Commission (National Policing Information Charges) Act 2016 (Cth)

Australian Privacy Principles
Freedom of Information Act 1982 (Cth)
Children and Young Persons (Care and Protection) Act 1998 NSW
Government Information (Public Access) Act 2009 NSW (GIPA)
Health Records and Information Privacy Act 2002 NSW (HRIP)
The National Police Checking Service (NPCS) Standards
NSW Child Safe Standards for Permanent Care

National Disability Insurance Scheme Act 2013
National Disability Insurance Scheme (Protection and Disclosure of Information - Commissioner) Rules 2018
Ombudsman Act 1974 NSW
Privacy Act 1998 (Cth)
Privacy and Personal Information Protection Act 1998 NSW
Public Interest Disclosures Act 1994 NSW
State Records Act 1998 NSW

Related policies, procedures and forms

Authority to Obtain and Release Personal Information Form
Code of Conduct
Duty of Care
Feedback and Complaints Management Policy
Feedback and Complaints Management Procedure
Information Security Policy
Media and Public Statements Policy
Media Consent Form
Referoo Privacy Statement
Release of Information Policy
Responding to a Breach of Privacy Procedure

Review

To be reviewed as per the Policy Review Schedule, or as legislation requires.

Document history

Revision Date	List of Changes	Author	Approval
2009	Policy developed v8		
11/09	New logo added v9		
06/11	Updated v10		
03/14	Updated v11		
04/16	Updated v12		
07/18	Updated v13		
08/18	National Criminal Check update – Anastasiya Holubko v14	AH	
06/11/18	Added Document Security – Anastasiya Holubko v15	AH	
03/04/19	NDIS and CPSL Legislation – Anastasiya Holubko v16	AH	
08/09/20	Anastasiya Holubko – update v 17	AH	

15/08/24	General review, remove NDIS references and conduct APP compliance check	LL	

Definitions

Agency – A collective term used for Marist180.

Client - A person participating in a program and receiving services provided by Marist180. The term includes NDIS Participants, Children, Young People and Adults.

Government Related Identifier – an identifier assigned by any government agency or a State or Territory authority. This includes Medicare numbers, Centrelink Reference numbers, driver licence numbers or Australian passport numbers.

People Manager - Anyone who manages people. The person in authority at a point in time, e.g. Area Manager, House Manager.

Personal Information - Any information that can be used to personally identify you. This may include but is not limited to your name, address, telephone number, email address and profession/occupation, health information or photographs of you. If the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered Personal Information.

Privacy and Confidentiality - The terms Privacy and Confidentiality are interchangeably used. Within this Policy, Confidentiality refers to ethical, legal and contractual duties not to misuse or disclose Confidential Information and Privacy refers to an obligation or right indicated in legislation that governs how Personal and Sensitive Information can be gathered, used and disclosed.

Sensitive Information - This is a subset of Personal Information that requires a higher level of Privacy protection because inappropriate handling of such information could adversely affect an individual. Examples include racial or ethnic origin, religious beliefs, sexual orientation, gender identity, gender expression, and intersexual status, details of case management, health or criminal record.

Staff - Includes employees [whether permanent, temporary or casual], carers, volunteers, contractors, consultants, agents, students undertaking work or professional experience.