



MARIST BROTHERS LINMEYER

EAST STREET, PO BOX 40, LINMEYER, 2105 † TELEPHONE: PRIMARY: 011 435 0646/7/8 - HIGH: 011 435 1100 † FAX, PRIMARY: 011 435 1708 - HIGH: 011 435 5886

INFORMATION PRIVACY POLICY AND FRAMEWORK (POPIA AND GDPR)

1. SCHEDULE	2
2. POLICY STATEMENT	2
3. DEFINITIONS OF TERMS USED IN THIS POLICY	2
4. PURPOSE AND SCOPE OF THE POLICY	3
5. PRIVACY COMPLIANCE FRAMEWORK.....	3
6. INFORMATION GOVERNANCE	5
7. INFORMATION PROCESSING PRINCIPLES	6
8. REVIEW OF POLICY.....	9

† LOVE OF WORK

† FAMILY SPIRIT

† IN THE WAY OF MARY

† SIMPLICITY

† PRESENCE



1. SCHEDULE

1.1	The Organisation	Marist Brothers Linmeyer
1.2	Registration number	465-468-NPO
1.3	VAT registration number	
1.4	Physical address	East Street, Linmeyer
1.5	Email address	twilliams@maristbl.co.za ; flawrence@maristbl.co.za

2. POLICY STATEMENT

- 2.1. Every person has rights with regard to how their personal information is handled and protected. In order to carry out its business and provide its services, the organisation set out in item 1 of the Schedule ("**Organisation**") may collect, store and process personal information about:
- 2.1.1. employees;
 - 2.1.2. customers;
 - 2.1.3. consumers;
 - 2.1.4. service providers / suppliers; and
 - 2.1.5. business contacts.
- 2.2. The Organisation recognises the need to treat this information in an appropriate and lawful manner. The Organisation is committed to complying with its obligations in this regard in respect of all personal information it handles, in a manner which maintains the confidence of the Organisation's customers, service providers / suppliers, business contacts and employees.
- 2.3. The Protection of Personal Information Act no. 4 of 2013 ("**POPIA**") and regulations (2018) relate to identifiable, living, natural persons and identifiable, existing, juristic persons. The European Union General Data Protection Regulation ("**GDPR**") only relates to the information of European Citizens (natural persons). Additional privacy legislation may also be applicable should the Organisation also conduct business in another country.
- 2.4. The types of information that the Organisation may be required to handle include details of current, past and prospective employees, service providers / suppliers, customers, consumers and other business contacts that the Organisation communicates with. The information would typically include names, addresses, email addresses, dates of birth, identity / passport numbers, phone numbers, private and confidential information and, potentially, special personal information. In addition, the Organisation may occasionally be required to collect and use certain additional types of personal information to comply with the requirements of the law.
- 2.5. The information may be stored on paper, electronically or by other media and is subject to certain legal safeguards specified in POPIA and GDPR, and potentially other applicable acts and regulations. The provisions of POPIA and GDPR impose restrictions on how the Organisation may collect and process the personal information in question.
- 2.6. This information privacy policy ("**Policy**") may be amended from time to time. Any breach of this Policy will be taken seriously by the Organisation and may result in disciplinary action being taken, which could include dismissal.

3. DEFINITIONS OF TERMS USED IN THIS POLICY

3.1. POPIA Definitions

- 3.1.1. "**data subject**" means all living, identifiable natural or juristic persons about whom the Organisation holds personal information or special personal information;
- 3.1.2. "**operator**" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- 3.1.3. "**personal information**" means information relating to an identifiable, living, natural or juristic person, including (i) factual information, such as identity and passport numbers, names, addresses, phone numbers, email addresses and the like, or (ii) opinions regarding a data subject, such as a performance appraisal;

- 3.1.4. **“processing POPIA”** means any operation or activity, whether or not by automatic means, concerning personal information, including the:
 - 3.1.4.1. collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information;
 - 3.1.4.2. dissemination of such information by means of transmission, distribution or making available in any other form; or
 - 3.1.4.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 3.1.5. **“responsible party”** means a public or private body, or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information; and
- 3.1.6. **“special personal information”** means more sensitive information about an individual that pertains to racial or ethnic origins, political, religious or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a data subject of an offence or any proceedings in respect of any offence allegedly committed by a data subject, which can only be processed under strict conditions and will usually require the express written consent of the data subject concerned).

3.2. **GDPR Definitions**

- 3.2.1. **“controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- 3.2.2. **“personal data”** means any information relating to an identified or identifiable natural person (“**data subject**”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and
- 3.2.3. **“processing GDPR”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and
- 3.2.4. **“processor”** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

4. **PURPOSE AND SCOPE OF THE POLICY**

- 4.1. This Policy sets out the Organisation’s general rules and the important legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of identifiable personal and special personal information.
- 4.2. This Policy also describes the privacy compliance framework and information governance of the Organisation in detail.
- 4.3. This Policy is applicable to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Organisation’s systems (“**Users**”).

5. **PRIVACY COMPLIANCE FRAMEWORK**

5.1. **BACKGROUND**

- 5.1.1. To ensure compliance with the requirements of relevant privacy legislation such as POPIA and GDPR, the focus areas that must be addressed to be compliant are as follows:
 - 5.1.1.1. governance;
 - 5.1.1.2. people;
 - 5.1.1.3. process; and
 - 5.1.1.4. technology.

5.2. **PRIVACY COMPLIANCE FRAMEWORK**

5.2.1. **Focus on governance**

- 5.2.1.1. The Organisation undertakes to take accountability for its actions by implementing good corporate governance.

5.2.1.2. The focus on governance means that the Organisation will establish an POPI Compliance Committee (“PCC”) and other structures to ensure that data protection compliance is an ongoing process and that continued management of information processes takes place.

5.2.2. Focus on process

5.2.2.1. The Organisation undertakes to implement processes to ensure that personal information is processed in line with relevant legislation.

5.2.2.2. This will include performing a Personal Information Impact Assessment (“PIIA”), as required by regulations promulgated under POPIA, and also developing and implementing the necessary policies and procedures and other control measures to ensure compliance with the relevant privacy legislation.

5.2.3. Focus on people

5.2.3.1. Most information security breaches involve people in one way or another. The Organisation undertakes to ensure that Users are made aware of their responsibilities in relation to processing personal information.

5.2.3.2. Users must undergo privacy and information security training at least annually and all new employees must be appropriately trained within 3 (Three) months of commencing employment with the Organisation.

5.2.4. Focus on technology

5.2.4.1. The Organisation undertakes to implement technology with appropriate security safeguards. The reference to “technology” includes software, hardware and data specific requirements. Appropriate security technological safeguards must be in place where personal information is processed, stored and destroyed. The Organisation undertakes to appoint a specialist in information technology (“IT”) to set up and manage the Organisation’s technology. This will be done either by in-house employees or by outsourcing this IT function to a compliant third party.

5.2.5. Review and audit

5.2.5.1. **Review and continuous monitoring:** The Organisation will ensure that the following is reviewed and monitored on an ongoing basis:

5.2.5.1.1. That the Organisation’s Governance Processes are functioning as intended;

5.2.5.1.2. That the Organisation’s processes have been reviewed on a regular basis and that all policies and procedures have been reviewed and updated at least annually;

5.2.5.1.3. That the Organisation’s other control measures that have been implemented are functioning as intended and that they are adequate and effective;

5.2.5.1.4. That the Organisation’s management and employees have been made aware and kept aware of how to process personal information and that a privacy awareness campaign has been developed and implemented;

5.2.5.1.5. That the Organisation’s safety and security technology areas have undergone annual vulnerability assessments and, where applicable, that penetration testing has been done. This also includes information security management.

5.2.5.2. Identify the gaps

5.2.5.2.1. On a regular basis, gaps or weaknesses (“Gap/s”) should be identified and actions to mitigate such Gaps should be recorded in a Privacy Implementation Action Plan (“PIAP”).

5.2.5.2.2. The Gaps should be prioritised and an accountable person should be appointed to rectify the Gaps.

5.2.5.2.3. A due date should be set by when the Gaps should be rectified.

5.2.5.3. Action the gaps

5.2.5.3.1. The Gaps should be actioned in accordance with the PIAP.

5.2.5.3.2. A specific responsible person should be identified to co-coordinate or perform an action and a due date to complete the action in question should also be set.

5.2.5.3.3. Where there is a specific due date set, the progress to address the Gaps should be reported to the IGC.

5.2.5.4. Audit the implementation

5.2.5.4.1. The Organisation undertakes to review the efficacy of the controls implemented to address and rectify the Gaps that have been identified.

5.2.5.4.2. The Organisation undertakes to ensure that the abovementioned review is conducted by an independent party not involved in the initial implementation. Where it is not possible to appoint an independent party within the Organisation then the review may be outsourced to independent third party auditors.

5.2.5.5. Assess the outcome

5.2.5.5.1. The Organisation undertakes to assess the outcome of the audit and determine what action must be taken, if any, to address the Gaps. Where the Gap has been addressed and rectified, it must be noted. Where there is additional work required to be done, it must be added to the PIAP.

5.2.5.6. Continuous reporting

5.2.5.6.1. The Organisation undertakes to continuously report the status of the management of personal information to the PCC and, at least on a quarterly basis, to the Board of Governors of the Organisation.

6. INFORMATION GOVERNANCE

6.1. INFORMATION OFFICER

6.1.1. The responsibilities of the information officer designated in terms of the POPIA include:

- 6.1.1.1. the encouragement of compliance, such as awareness and training, by the Organisation, taking into consideration all of the conditions for the lawful processing of personal information;
- 6.1.1.2. ensuring compliance by the Organisation with the provisions of POPIA;
- 6.1.1.3. dealing with requests made to the Organisation in terms of POPIA, such as requests made from data subjects to update or view their personal information;
- 6.1.1.4. working with the information regulator (“**Regulator**”) in relation to investigations; and
- 6.1.1.5. the designation and delegation of relevant duties to deputy information officers appointed by the Organisation.

6.1.2. The responsibilities of the information officer have been expanded upon in the regulations promulgated under POPIA on 14 December 2018. In this regard, the information officer must ensure that:

- 6.1.2.1. a compliance framework is developed, implemented, monitored and maintained;
- 6.1.2.2. a PIIA is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- 6.1.2.3. a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000;
- 6.1.2.4. internal measures are developed, together with adequate systems, to process requests for information or access thereto; and
- 6.1.2.5. internal awareness sessions are conducted regarding (i) the provisions of POPIA, (ii) regulations promulgated in terms of POPIA, (iii) relevant industry codes of conduct, or (iv) information obtained from the Regulator.

6.2. INFORMATION GOVERNANCE COMMITTEE RESPONSIBILITIES

6.2.1. **Strategic:** The oversight of the full information lifecycle for both structured and unstructured information, including:

- 6.2.1.1. endorsement of information policies, principles and procedures in relation to information management;
- 6.2.1.2. assisting with ensuring compliance with the provisions of POPIA and GDPR, where applicable, which include the following:
 - 6.2.1.2.1. The security and integrity of data/information held by, or on behalf of, the Organisation;
 - 6.2.1.2.2. The dissemination of the Organisation’s data/information to third parties;
 - 6.2.1.2.3. Information and data confidentiality and availability;
 - 6.2.1.2.4. Information and data quality, including completeness, accuracy and ensuring that information is up to date;
 - 6.2.1.2.5. Information sharing arrangements with other parties;
 - 6.2.1.2.6. Retention and destruction of information practices;
 - 6.2.1.2.7. Document management, including the digitisation of documents; and
 - 6.2.1.2.8. Discussing and identifying the areas where consent will be needed for the processing of personal information.
- 6.2.1.3. assisting with the integration of people, technologies, information and processes across the Organisation;
- 6.2.1.4. identifying and assessing the information risks and provide input to the Organisation’s enterprise wide risk management process;
- 6.2.1.5. ensuring that there is proactive monitoring of data/information breach incidents and review the response to these incidents;
- 6.2.1.6. reviewing and provide oversight to ensure that the information architecture supports confidentiality, integrity and availability of information;
- 6.2.1.7. endorsing information-related strategies and roadmaps;
- 6.2.1.8. prioritising information-related initiatives;

- 6.2.1.9. establishing information-related metrics and oversight of results;
 - 6.2.1.10. directing efforts to resolve issues in relation to information management;
 - 6.2.1.11. assisting with advice on the leverage of information to sustain and enhance the Organisation's intellectual capital; and
 - 6.2.1.12. reviewing and assessing the actions taken to monitor the effectiveness of information management and how the outcomes were addressed.
- 6.2.2. **Operational:** The PCC will:
- 6.2.2.1. establish structures needed to support information governance in the Organisation;
 - 6.2.2.2. delegate authorities for the implementation of decisions;
 - 6.2.2.3. co-ordinate information management responsibilities across the Organisation to ensure complete coverage of the information lifecycle;
 - 6.2.2.4. make the Users aware of the PCC and its roles and responsibilities;
 - 6.2.2.5. promote good information management practices and publish the names of the Information Asset Owners ("IAO's") for easy reference so they can be notified of particular issues relating to their domain; and
 - 6.2.2.6. train and mentor IAOs to enable them to fulfil their roles.

7. INFORMATION PROCESSING PRINCIPLES

- 7.1. **POPIA:** The Organisation fully supports and complies with the 8 (Eight) protection principles of POPIA which are summarised below:
- 7.1.1. **Accountability:** a responsible party must ensure that the information processing principles are complied with;
 - 7.1.2. **Processing limitation:** personal information must be processed lawfully and in a reasonable manner;
 - 7.1.3. **Purpose specification:** personal information must be obtained/ processed for specific lawful purposes;
 - 7.1.4. **Further processing limitation:** further processing of personal information must be in accordance or compatible with the purpose/s for which it was originally collected;
 - 7.1.5. **Information quality:** personal information must be complete, accurate, not misleading and kept up to date;
 - 7.1.6. **Openness:** personal information may only be processed by a responsible party who has taken reasonable steps to notify the data subject;
 - 7.1.7. **Security safeguards:** personal information must be kept secure, and its confidentiality and integrity must be maintained; and
 - 7.1.8. **Data subject participation:** a data subject has the right to request the responsible party to confirm, free of charge, whether or not the responsible party holds personal information, together with a description of the personal information held by such responsible party.
- 7.2. **ACCOUNTABILITY**
- 7.2.1. The provisions of POPIA are intended not to prevent the processing of personal information, but to make sure that a responsible party ensures that the information processing principles as set out in POPIA, and all the measures that give effect to the principles, are complied with.
 - 7.2.2. The data subject must be told the identity of the responsible party (in this case, the Organisation) and the purpose for which personal information is to be processed by the Organisation.
 - 7.2.3. This Policy, developed by the Organisation to protect privacy, is available at the Organisation premises and is also accessible online at the Organisation's website. This Policy outlines the Organisation's commitment to privacy.
- 7.3. **PROCESSING LIMITATION**
- 7.3.1. For personal information to be processed lawfully, certain conditions have to be met. These may include, amongst other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. When special personal information is being processed, in most cases the data subject's explicit consent to the processing of such special personal information will be required.
 - 7.3.2. A responsible party must collect personal information directly from the data subject unless (i) information is in a public record, (ii) the data subject has consented, (iii) the collection of personal information does not prejudice the legitimate interest of the data subject, or (iv) collection is necessary to comply with, or to avoid prejudice with or to the maintenance of, laws; to enforce legislation concerning the collection of revenue; for purposes of proceedings in a court; or in the interest of national security.
 - 7.3.3. Where the Organisation processes personal information as a responsible party, the data subject should be informed of this fact. The data subject should also be informed for what purpose the personal information is being processed by the Organisation, and where or to whom such personal information may be disclosed or transferred. The Organisation

has drafted a "Terms of Use" document which can be found online at the Organisation's website, which explicitly outlines how and in what circumstances the Organisation may use a person's information.

7.4. PURPOSE SPECIFICATION

- 7.4.1. Personal information may only be processed for a specific and lawful purpose, or for any other purpose specifically permitted by POPIA, and steps must be taken to ensure that the data subject is aware of the purpose of the collection of the personal information. The Organisation undertakes not to (i) collect personal information for one purpose and then use the personal information for another purpose, or (ii) retain personal information for any longer than is necessary for achieving the purpose for which the information was collected.
- 7.4.2. Personal information should only be collected to the extent that it is required for the specific purpose communicated to the data subject. Any personal information which is not necessary for that purpose should and will not be collected by the Organisation.
- 7.4.3. If it becomes necessary to change the purpose for which the personal information is processed, the data subject will be informed of the new purpose before any processing occurs. Any employee personal information collected by the Organisation will be used for ordinary human resources purposes. Where there is a need to collect employee personal information for any other purpose, the Organisation will notify the employee in question of this and, where it is appropriate and practicable, the Organisation will get the employee's consent prior to such processing.
- 7.4.4. Where the Organisation collects personal information directly from a data subject, the personal information collected and processed by the Organisation, such as identity number, proof of address and the like, will only be used for the required purpose.

7.5. FURTHER PROCESSING LIMITATION

- 7.5.1. Personal information should not be kept longer than is necessary for the purpose for which it was collected. For guidance in relation to a particular personal information retention period, a User should contact the Organisation. The Organisation has various legal obligations to keep certain personal information of Users for a specified period of time. In addition, the Organisation may need to retain personal information for a period of time to protect its legitimate commercial and other interests.
- 7.5.2. The Organisation will not use any personal information for any purpose other than that for which it received the information in the first place, unless any further processing of such information is compatible with the original purposes for which the information was collected.

7.6. INFORMATION QUALITY

- 7.6.1. Personal information must be complete, accurate, and kept up to date. Personal information which is incorrect or misleading is not accurate and steps will be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal information will be destroyed. Employees should ensure that they notify their manager / human resources of any relevant changes to their personal information so that it can be updated and maintained accurately.
- 7.6.2. All personal information which is in paper form should be destroyed only by shredding. If the personal information is held electronically, the Organisation must ensure that a reputable service provider destroys the personal information so that there is no future record of the information and the Organisation must obtain an undertaking from the applicable service provider in this regard.

7.7. OPENNESS

- 7.7.1. Personal information may only be processed by the Organisation if the Organisation has notified the data subject that the Organisation has obtained the information from legitimate sources.
- 7.7.2. In cases where the Organisation works directly with a data subject, the Organisation will take reasonable, practicable steps to ensure that the data subject is aware of the following:
 - 7.7.2.1. What information is being collected and, where it is not collected from the data subject, the source of the information;
 - 7.7.2.2. The full name and addresses of the Organisation;
 - 7.7.2.3. The purpose for which the information is being collected;
 - 7.7.2.4. Whether supplying the personal information to the Organisation is voluntary or mandatory;
 - 7.7.2.5. The consequences of failure to provide the information;
 - 7.7.2.6. The applicable law authorising or requiring the collection of the information;
 - 7.7.2.7. The right to lodge a complaint against the Organisation the Regulator; and
 - 7.7.2.8. Any further relevant information, such as recipient or category of recipients of information, nature of information, existence of the right of access and the right to rectify information collection.

7.8. SECURITY SAFEGUARDS

- 7.8.1. The Organisation and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information.
- 7.8.2. The Organisation will put in place procedures and technologies to maintain the security of all personal information. Personal Information may only be transferred to an operator if the operator has agreed to comply with those procedures and policies or has adequate security measures in place.
- 7.8.3. Users may refer to the Organisation's information security and related policies for further information concerning the Organisation's security safeguards.
- 7.8.4. The following principles must be maintained by the Organisation:
 - 7.8.4.1. **Confidentiality:** that only people who are authorised to use the personal information in question can access it. The Organisation will ensure that only authorised persons have access to an employee's personnel file and any other personal or special information held by the Organisation. Employees are required to maintain the confidentiality of any personal information and / or special personal information that they have access to.
 - 7.8.4.2. **Integrity:** that proper security safeguards are in place to ensure the maintenance and assurance, of the accuracy and consistency of information / data over its entire life cycle.
 - 7.8.4.3. **Availability:** that authorised users should be able to access the personal information if they need it for an authorised purpose.
- 7.8.5. Examples of security procedures at the Organisation include:
 - 7.8.5.1. Secure lockable desks and Cupboards – desks and cupboards must be kept locked if they hold confidential personal identifiable information of any kind;
 - 7.8.5.2. Methods of Disposal – paper documents must be shredded. CD ROMs and USB keys should be physically destroyed when they are no longer required;
 - 7.8.5.3. Equipment – data users must ensure that individual computer monitors do not show confidential information to passers-by and that they log off from their computer when it is left unattended; and
 - 7.8.5.4. User Management – any access to the Organisation's database is logged by the Organisation through a username and password system. Any changes / updates / uploads to the system are constantly tracked.
- 7.8.6. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Organisation or any third party processing personal information under the authority of the Organisation, must notify the Regulator and the data subject as soon as is reasonably possible, taking into consideration the time that is taken by the Organisation to determine the scope of the breach and to restore the integrity of its information systems.
- 7.8.7. Any notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:
 - 7.8.7.1. Mailed to the data subjects last known physical or postal address;
 - 7.8.7.2. Sent by email to the data subjects last known email address;
 - 7.8.7.3. Placed in a prominent position on the website of the Organisation;
 - 7.8.7.4. Published in the news media; or
 - 7.8.7.5. As directed by the Regulator.
- 7.8.8. The notification referred to above must provide sufficient information to all the affected data subjects to take protective measures against the potential consequences of the security compromise including:
 - 7.8.8.1. a description of the possible consequences of the security compromise;
 - 7.8.8.2. a description of the measures that the Organisation intends to take or has taken to address the security compromise;
 - 7.8.8.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
 - 7.8.8.4. if known to the Organisation, the identity of the unauthorised person who may have accessed or acquired the personal information in question.

7.9. DATA SUBJECT PARTICIPATION

- 7.9.1. A formal request from a data subject for information that the Organisation holds about them must be made in writing, accompanied with adequate proof of identification (in most instances, a certified copy of the individual's identity document or passport and proof of residence will be sufficient).
- 7.9.2. Any employees who receive a written request in respect of data held by the Organisation must forward it to the information officer immediately.
- 7.9.3. Any individual requesting personal information that may be held by the Organisation will be referred by the relevant employee to whom the request was made to the information officer, who will process the request. The information

officer will either process the request directly, or will direct such employee to request a certified copy of the individual's identity document or passport as well as proof of address. Once this is received, the employee will then be authorised to release the personal information to the individual. The employee must:


- 7.9.3.1. record the request in the request register / system; and
- 7.9.3.2. safely store the certified copy of the identity document and passport either in a file in a locked cupboard (if in paper format) or online in an encrypted folder which cannot be accessed by unauthorised personnel. Storage of these documents should be kept for 1 (one) year, after which they must be properly destroyed.
- 7.9.4. Any employee dealing with telephonic enquiries from data subjects should guard against disclosing any personal information held by the Organisation over the phone. In particular, the employee must:
 - 7.9.4.1. check the identity of the caller to ensure that information will only be given to a person who is entitled to that information – this can be accomplished by confirming: identity number, date of birth, address, cell phone number and the like;
 - 7.9.4.2. request that the caller put their request in writing if the employee is not completely sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified. In these circumstances, the employee should also request that a certified copy of the identity document / passport of the individual is provided before information is released;
 - 7.9.4.3. refer the request to their manager for assistance in difficult situations. No employee should feel forced to disclose personal information; and
 - 7.9.4.4. where a request has been made in terms of this section, and personal information is communicated to the data subject, the data subject must be advised of their right to request the correction of the information.
- 7.9.5. The data subject may request that the Organisation correct or delete personal information which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or to destroy such record of personal information. If such a request is made, the Organisation must send this request to the appropriate party within the Organisation who should then correct the information, destroy or delete it, and provide the data subject with credible evidence that this has been done.

7.10. GDPR

- 7.10.1. The Organisation fully supports and complies with the 6 (Six) protection principles of the GDPR which are summarised below:
 - 7.10.1.1. **Lawfulness, fairness and transparency:** The personal information of the European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
 - 7.10.1.2. **Purpose limitation:** The personal information of the European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.
 - 7.10.1.3. **Data Minimisation:** The personal information of the European citizens will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - 7.10.1.4. **Accuracy:** The personal information of the European citizens will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.
 - 7.10.1.5. **Storage Limitation:** The personal information of the European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
 - 7.10.1.6. **Integrity and Confidentiality:** The personal information of the European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. REVIEW OF POLICY

The Organisation will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, taking into account changes in the law and organisational or security changes.

 Marist Brothers Linmeyer	Marist Brothers Linmeyer	
	Author: Marist Brothers Linmeyer Authorised: Exco Date revised: Revision: 1 Policy No: MBL3001	<u>Policy Title:</u> Information Privacy Policy and Framework (Popia and GDPR)