Privacy Policy

Section 1 - Purpose

(1) This policy sets out key points about how the Catholic Diocese of Maitland-Newcastle (the Diocese), including its agencies, handles personal information.

(2) The Diocese collects, holds, gives access to, uses, discloses, and corrects personal information to carry out its many functions and activities and, in doing so, is bound by the Privacy Act 1988 (Cth) (Privacy Act) and the Australian Privacy Principles (APPs).

(3) The Diocese also collects, holds, uses and discloses health information and is bound by the Health Records and Information Privacy Act 2002 (NSW)(HRIPA), the Health Privacy Principles (HPPs) MyHealth Records Act 2012 (Cth)(MHR) and Healthcare Identifiers Act 2010(Cth)(HI) when handling personal information which is health information.

(4) The Diocese complies with the Privacy and Personal Information Protection Act 1998 (NSW)(PPIPA) and the Government Information (Public Access) Act 2009 (NSW)(GIPA) where required under state government contracts. The Diocese will comply with any direction from the NSW government agency from which it receives funding with respect to compliance with Privacy Laws.

(5) This policy and its related policy documents establish, implement, and maintain privacy processes and provide the steps required to meet these ongoing compliance obligations.

Section 2 - Policy Statement

(6) The Diocese respects and values the personal information and health information that it is entrusted with.

(7) The Diocese is committed to:

a. practicing good privacy governance and meeting its ongoing compliance obligations; and
b. ensure that personal information is managed openly and transparently by implementing practices, procedures, and systems to ensure compliance with the Australian Privacy Principles.

Section 3 - Scope

(8) All personal information and health information collected, held, and used by the Diocese must be managed in accordance with this policy and the related policy documents.

(9) This policy applies to all workers of the Diocese including its agencies. This policy also applies to parishes if decreed by the Bishop.

(10) This policy also applies to other persons conducting services for the Diocese who have access to information held by the Diocese.

(11) Everyone in the Diocese who manages records and information is accountable for ensuring privacy is respected and protected.

(12) This policy should be read in conjunction with privacy procedures applicable to agencies' operations.

Section 4 - Policy Principles

Types of Personal Information Collected and How it is Collected

(13) The Diocese carries out a multitude of functions, services, and activities. The Diocese provides faith, spiritual, pastoral, educational, social welfare, housing and community development through its parishes and agencies.

(14) The Diocese will only collect relevant personal information for a lawful purpose and by lawful means where it is reasonably necessary to enable the Diocese to carry out its mission, activities, functions and ministries or to assist persons should they have an inquiry.

(15) The Diocese endeavours to ensure that the information collected will be accurate, up-to-date, complete and not excessive.

(16) The Diocese collects and holds personal information, which may include sensitive information and health information about:

a. children, which may be related to children receiving sacraments or pastoral care, a child's enrolment at a diocesan school, after-school care facility or sporting association;
b. adults receiving sacraments or pastoral care and witnesses to sacraments;
c. people we support in community programs, counselling and clinical support, National Disability Insurance Scheme services, child, youth and family services and social enterprises;
d. applicants for and people living in housing owned and managed by the Diocese or its agencies;
e. staff, workers and clergy;
f. job applicants, volunteers, contractors, and suppliers;
g. people involved in fundraising and relationship building, including banking or other payment details;
h. people we communicate with or who attend Mass, liturgies, seminars or events;
i. people who are members of groups, organisations, societies, institutes of apostolic life or the Church community;
j. people who have access to and use the Diocese websites and other electronic media and communications;
k. parents or guardians of those we hold personal information about; and
l. other persons related to these activities, e.g. carers, grandparents, etc.

(17) Information collected may include (but is not limited to) a person's name, contact details, date of birth, email address, medical information, applications for employment and supporting documents, employment contracts, records relating to the payment of wages, employment benefits and leave, training and development information, information about an employee's performance, occupation, family background, religion, citizenship and visa information, school results, conduct, complaint or behaviour records, counselling reports, Family Court orders, information about referrals to government agencies, photos and videos at events, and in some cases, financial records.

(18) The Diocese will take steps to make sure the person is aware of the information being collected, why it's being collected, and who will be using and storing it. This may include providing a Privacy Collection Notice, copy, or electronic link to this policy. Should the Diocese need to collect, use and disclose a worker’s personal and health information to facilitate their return to work and recovery as part of managing or processing a workers compensation claim, the Diocese will obtain the worker’s valid consent. For further information on this please refer to the Diocese’s

Return to Work Program.

(19) Personal information is generally collected from a person or their authorised representative through forms filled out by the person or their guardian/responsible person, face-to-face meetings, interviews, telephone calls, and websites or other electronic data.

(20) In some circumstances, a third party, including other parishes or schools, may provide the Diocese with personal information, e.g., a reference about an applicant for a position, personal information from a student's previous school to facilitate the transfer of a student to a Diocese school, information we collect from people we help or educate, information from third party information providers or people responding to our inquiries. The Diocese also collects and receives Personal and Health Information from third parties such as other regulatory agencies, and government authorities, including for example the Diocese's workers compensation insurer and claims administrators, or direct from medical practitioners treating employees.

(21) We may also collect personal information through surveillance activities (such as CCTV security cameras) and monitoring of email and social media accounts managed within the Diocese's information networks.

(22) In some cases, where a person does not provide the personal information the Diocese requests, we may not be able to help, employ, engage with, educate or minister to that person in some or any of the Diocese's activities.

(23) A person may also choose to deal with the Diocese anonymously or use a pseudonym (where lawful and practical). However, the Diocese will need to identify a person in many circumstances, e.g., to administer certain sacraments, provide care for children, or process a job or volunteer application.

Unsolicited Personal Information

(24) Where the Diocese receives unsolicited information, the Diocese will determine whether it could have been collected separately under the Australian Privacy Principles within a reasonable period.

(25) If it is determined that the personal information could have been collected lawfully, then the rest of the Australian Privacy Principles apply as if the information had been collected in that manner.

(26) If it is determined that the information could not have been collected lawfully, it will be destroyed or de-identified where it is otherwise lawful to do so.

Use and Disclosure of Personal Information

(27) The Diocese uses personal information it collects to:

a. administer the sacraments and pastoral care;
b. keep people informed about matters relating to spiritual life through correspondence and newsletters;
c. look after a person's spiritual and physical wellbeing;
d. keep people informed about matters relating to their child's schooling through correspondence and newsletters;
e. provide care for a child(ren) under the Diocese's supervision (including education, social, spiritual, and medical wellbeing);
f. fundraise, seek, and administer donations;
g. tell people about events, services and developments in the Church and our community;
h. assess a job or volunteer application;
i. determine eligibility for housing services;
j. manage staff and volunteers;
k. ensure appropriate provision of services; and

l. satisfy the Diocese's legal obligations and allow the Diocese to discharge its duty of care;
m. manage work, health and saftey needs of employees; and
n. manage and process workers compensation claims

(28) The Diocese normally only uses or discloses personal information for the reason the Diocese collected it unless disclosure is permitted under other circumstances, including if required by law.

(29) In particular circumstances, the Diocese may disclose personal information, including sensitive information held about a person, including as follows:

a. with consent from the person for a purpose other than the purpose for which it was collected;
b. for a secondary purpose related to the primary purpose, which the person would reasonably expect;
c. where it is reasonably believed that the disclosure is necessary for an enforcement related purpose;
d. if the information is needed to deal with a serious risk of harm;
e. for educational, care and administrative purposes and to seek support and advice;
f. for assessment and educational authorities;
g. to agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes;
h. to government departments, including for policy and funding purposes and to:
    i. the applicable NSW government agency for agency audits or assessments of the organisation's compliance with the Human Services Agreement; or
    ii. the applicable NSW government agency if the agency requests information to comply with its obligations under the Government Information (Public Access) Act 2009 (NSW).
i. to medical practitioners;
j. within the Diocese:
    i. to people providing services to the Diocese, including volunteers and third-party service providers;
    ii. to recipients of the Diocese publications;
    iii. to parents and/or guardians; and
    iv. to providers of information management and storage systems and other information technology services.
k. if required or authorised by an Australian law or court/tribunal order, including child protection laws;
l. to anyone to whom the person authorises the Diocese to disclose information;
m. where the use or disclosure is permitted by an exception under Australian Privacy Principle 6.2 or 6.3; and
n. to the workers compensation insurer and claims administrators.

(30) If personal information is disclosed for enforcement related activities by an enforcement body (e.g., the police), a written record of that disclosure will be made.

(31) Any request for personal information made by an enforcement body must:

a. be made in writing as evidence to justify that disclosure is required; and
b. be approved by the Diocese Governance Team.

(32) When the Diocese has entered into contracts or agreements with any external parties or has outsourced any function or activity, appropriate clauses must be added to comply with the relevant Privacy laws.

Overseas Disclosures

(33) The Diocese may disclose personal information to third-party suppliers and service providers located overseas,

including data hosting and IT cloud service providers such as Microsoft 365, to enable authentication and provide technical support. We will take reasonable steps to ensure that the overseas recipients of personal information do not breach the privacy obligations relating to the personal information.

(34) The Diocese will disclose personal information about a person or their child outside Australia where they have requested this. When making a request, it is agreed and acknowledged that the Diocese will have no control over the information that it discloses and that the Diocese will not be able to ensure that the overseas recipient handles that information in accordance with the Privacy Act, the Australian Privacy Principles, and any other applicable Australian laws.

(35) If consent is given for the disclosure and the overseas recipient handles the personal information in breach of the APPs:

a. the Diocese will not be accountable under the Privacy Act; and
b. the person will not be able to seek redress under the Privacy Act.

(36) Examples relevant to clause 35 include:

a. the publication on the internet of material that may contain personal information such as photographs, video and audio recordings, and posts and comments on the Diocese's social media platforms;
b. the provision of personal information to facilitate educational outcomes, e.g., school exchange;
c. the provision of personal information to recipients using a web-based email account where data is stored on an overseas server; and
d. the provision of personal information to foreign governments and law enforcement agencies (in limited circumstances and where authorised by law).

(37) If the Diocese outsources data services to a third-party provider based overseas (such as a server provider in another country), the Diocese will:

a. take reasonable steps to make sure that the third-party provider does not breach the Australian Privacy Principles; and
b. state in which countries the personal information is likely to be stored.

Access and Correcting Personal Information

(38) The Diocese endeavours to ensure that the personal information held is accurate, complete, up-to-date and not misleading.

(39) The Diocese will also take reasonable steps to correct information it holds if it considers the information incorrect.

(40) A person may access any personal information that is held about them. Parents can generally make such a request on behalf of their children. Guardians can generally make such a request on behalf of a person under their guardianship. A request for access should be put in writing and sent to the Diocese using the details in Section 6 below.

(41) The Diocese will respond within a reasonable period after a request for access is made by either agreeing to or refusing to give access.

(42) The Diocese may require a person requesting access to personal information to verify their identity and specify what information is required before providing access. In some circumstances, as provided by Australian Privacy Principle 12, the Diocese may be unable to provide access; in this case, the person will be notified in writing with an explanation of why and how they can take the matter further.

(43) The Diocese will not charge a person for making a request; however, the Diocese may charge reasonable costs for providing access to any information requested.

(44) A person may seek to update the personal information held about them by contacting the Diocese at any time using the details in Section 7 below. If the Diocese is unable to correct the information, we will give notice in writing and explain why and how the matter can be taken further. A statement associated with the information believed to be inaccurate, out-of-date, incomplete, irrelevant or misleading can be requested.

Deletion of personal information

(45) The Diocese will take reasonable steps to destroy or de-identify information it holds where it no longer needs the information for any purpose for which it was used or disclosed, and it is not required under another law, court or tribunal order.

Consent and Right of Access to the Personal Information of Children

(46) The Diocese will assess whether a child has the capacity to make their own privacy decisions on a case-by-case basis with regard to matters such as their age and circumstances. Generally, persons over 15 years old will have the capacity to make their own privacy decisions.

(47) For children under 15 years or who otherwise do not have the capacity to make these decisions for themselves, The Diocese will refer any requests for consent and notices in relation to personal information to the parent and/or guardian. We will treat consent given by a parent and/or guardian as consent given on behalf of the child or person subject to guardianship, and notices to parent and/or guardians will act as notice given to the child or person subject to guardianship.

(48) The Diocese respects the rights of parents and/or guardians to make decisions concerning their child's education.

(49) Parents may seek access to personal information held by a Diocesan school about them or their child by contacting the school principal in writing. However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where a school believes that the student has the capacity to consent and the school is not permitted to disclose information to the parent without the student's consent, where the release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the student.

(50) A Diocesan school may, at its discretion, on the request of a student, grant the student access to information held by the school about them or allow a student to give or withhold consent to use of their personal information, independently of their parents and/or guardians. This would normally be done only when the maturity of the student and/or the student's circumstances warrant it.

Out-of-home care

(51) The Diocese will allow access, free of charge, to personal information for a child or person who is leaving or has left out-of-home care to any records kept by a Diocese agency or authorised carer.

(52) The Diocesan agency must provide an appropriate person to support and assist the person seeking access to information at the time when access to the information occurs. The information is to be provided orally or in writing, as requested by the child or person concerned.

(53) A child(ren) and young people in out-of-home care also have the right to request, access, read and add to the information kept about them.

Direct Marketing

(54) The Diocese may, from time to time, engage in direct marketing activities for various purposes, such as fundraising and providing information about our services that we consider may be of interest.

(55) The Diocese will not provide personal information to other organisations for the purposes of direct marketing.

(56) The Diocese will only use or disclose sensitive information (including health information) for direct marketing if a person has consented to that use or disclosure.

(57) The Diocese may use or disclose non-sensitive personal information for direct marketing if the following conditions are met:

a. the information was collected directly from the person;
b. the person whose information is disclosed would reasonably expect it to be used for direct marketing; and
c. an easy 'opt-out' option is provided for anyone who doesn't want to receive direct marketing and the person has not chosen to opt out.

(58) These communications may be sent in various forms, e.g., mail, SMS, and email, in accordance with applicable marketing laws, such as the Spam Act 2003(Cth).

(59) If a preference for a particular method of communication is indicated, The Diocese will endeavour to use that method whenever practical to do so. In addition, at any time, a person may opt-out of receiving marketing communications from the Diocese by contacting the Diocese using the details in section 6 below or by using the opt-out facilities provided in the marketing communications, and we will then ensure that their name is removed from the mailing list.

Security of Personal Information

(60) Users of the Diocese information and communication technology (ICT) systems are required to respect the confidentiality of personal information and the privacy of persons.

(61) Access to personal information in the Diocese is restricted to those who require access.

(62) The Diocese has processes in place to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure by using various methods, including locked storage of paper records and password-restricted access rights to computerised records.

(63) The Diocese has ICT security systems, policies, procedures, processes, and controls designed to protect personal information stored on our computer networks.

(64) Where the Diocese uses internet (or cloud) based storage systems, it will take reasonable steps to ensure third-party storage providers comply with the Privacy Laws.

(65) Where the Diocese no longer requires personal information for a purpose required under the Privacy Act, the Diocese will take reasonable action to destroy or de-identify that information unless it would be unlawful for us to do so.

(66) The Diocese has policies and procedures, including email and internet usage, confidentiality and document security policies designed to ensure ICT users follow correct protocols when handling personal information.

(67) ICT users receive training on the uses of the Diocese ICT systems about data security and ensuring users are aware of their obligations in relation to privacy and ICT systems.

(68) Due diligence with respect to third-party service providers who may have access to personal information is undertaken, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

(69) Where personal information is stored in hard copy records, these records are kept in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need-to-know basis.

(70) Physical security measures are implemented around buildings and grounds to prevent break-ins.

Data Breach and Breach of Privacy Laws

(71) The Diocese has a Data Breach Response Plan that outlines the steps to take and the people responsible for responding to a data breach.

(72) If it is suspected that an 'eligible data breach' has occurred and there is a real risk of serious harm to a person/s as a result of the breach, the Diocese is required to notify both the person affected and the Office of the Australian Information Commissioner as soon as possible by completing a incident report.

(73) The Diocese is obliged to notify the applicable NSW government agency immediately if it has reasonable grounds to believe there has been a breach of the Privacy Laws in connection with the delivery of Services under a Human Services Agreement.

Health Record Linkage Systems

(74) The Diocese will only use health records linkage systems (such as MyHealth Record) with consent.

Section 5 - Enquiries and Complaints

(75) For further information about how the Diocese manages personal information, please get in touch with the Diocese using the details in Section 6.

(76) If it is believed that the Diocese has acted contrary to this Policy or the Privacy Laws, please lodge a complaint in writing using the Submit feedback or complaint link or email provided in Section 6.

(77) If a person makes a privacy complaint, the Diocese will acknowledge receipt of the complaint, undertake inquiries and provide a response to the person within 30 days.

(78) If not satisfied with the response, the person can contact the Office of the Australian Information Commissioner (OAIC) by phone at 1300 363 992 to query privacy rights or visit www.oaic.gov.au for more information about how to lodge a complaint with OAIC. The OAIC has the power to investigate the matter and make a determination.

Section 6 - Contact Details

(79) The Diocese complaint management service is located at 841 Hunter Street, Newcastle West 2302

(80) You can submit feedback or complaints by:

a. clicking this link to submit a feedback or complaint;
b. phoning 1300 461 831; or
c. emailing feedback@mn.catholic.org.au

(81) Further information can be found on our website under Complaints and Feedback.

Section 7 - Consequences of Breaching this Policy

(82) Any worker found to be in breach of this Policy may be subject to disciplinary action, including dismissal where a serious breach occurs.

Section 8 - Notations

(83) If there is any inconsistency between a policy document in existence before the commencement of this policy and a policy document developed after the commencement of this policy, the latter applies to the extent of the inconsistency.

Section 9 - Document Review

(84) This policy will be reviewed when there is a legislative change, organisational change, delegation change, or technology change or at least every three years to ensure it continues to be current and effective.

Status and Details

Status	Current
Effective Date	20th February 2024
Review Date	5th September 2026
Approval Authority	Chief Executive Officer
Approval Date	5th September 2023
Expiry Date	To Be Advised
Unit Head	Megan Grainger Chief Governance Officer
Enquiries Contact	Governance

Glossary Terms and Definitions

"Bishop" - Is defined in the Roman Catholic Church Trust Property Act 1936 (NSW) being a person for the time being administering the Diocese, whether as Archbishop or Bishop, Coadjutor Archbishop, Vicar Capitular or Administrator.

"Parishes" - Is the local parish as defined by its geographical boundaries. "… is a certain community of the Christian faithful stably constituted in a particular church, whose pastoral care is entrusted to a pastor (parochus) as its proper pastor (pastor) under the authority of the diocesan bishop." (Can. 515§1)

"Direct marketing" - Is communicating with a person to promote goods and services and can include fundraising.

"Health information" - Means personal information that is information or an opinion about the physical or mental health or a disability (at any time) of a person, or a person's express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to a person, or other personal information collected to provide, or in providing, a health service. For a full definition see section 6 of the Health Records and Information Privacy Act 2002 (NSW).

"Personal information" - Information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or reasonably identifiable, from the information or opinion. This includes sensitive information.

"Sensitive information" - Means information or an opinion that is also personal information, about a person's racial or ethnic origin, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practices, criminal history, health information, and genetic and biometric information. This information must be protected due to its confidentiality or availability requirements because if exposed it could lead to harm or privacy/data breaches.

"Unsolicited information" - Is personal, sensitive or health information that you have received that you took no active steps to collect.

"Complaint management service" - The diocesan service provided by Governance that is dedicated to the resolution of complaints and includes: • Resolution Officers who have an impartial, facilitative, and supportive role in the resolution of complaints at the Agency, and • Administrative Review Officers who may be allocated to finalise a complaint by the completion of an Administrative Inquiry.

"Incident report" - An online incident report form in mnResponse that is to be completed as soon as practicable after an injury, illness, incident, near miss or hazard is reported, whether or not there has been a claim for compensation.

"Agency" - Diocesan agencies may also be referred to as directorates. Diocesan agencies are intra-diocesan organisational structures that have been established and developed in the life of the church, to undertake good works and services on behalf of the Diocese and have the capacity to bind the Diocese to its actions. For the most part, but not exclusively, diocesan agencies are led by executive directors. Examples of Diocesan agencies include: • CatholicCare Social Services Hunter-Manning; • Catholic Community Fund (including Catholic Development Fund Maitland-Newcastle (CDFMN)); • Catholic Schools and the diocesan systemic schools; • Hunter Community Housing; • St Nicholas services including Early Education centres and Out of School Hours Care (OOSH) services; and • Shared Services, which is inclusive of multiple specialist tertiary providers to diocesan parishes and agencies, that forms part of the Diocesan Curia.

"Catholic Diocese of Maitland-Newcastle (the Diocese)" - The Catholic Diocese of Maitland-Newcastle (the Diocese) is inclusive of all parishes and agencies, communities, ministries and works that are under the authority of the Bishop of Maitland-Newcastle. The Bishop takes his authority from Canon Law (Canons 375-402). The geographical coverage of the Diocese includes all or part of the Newcastle, Lake Macquarie, Maitland, Cessnock, Port Stephens, Singleton, Muswellbrook, Upper Hunter, Dungog and Mid-Coast local government areas, with almost 160,000 Catholics, 38 parishes and serviced by multiple diocesan ministries and agencies. The Diocese is not wholly geographic in nature. There are elements of the Catholic Church operating within the physical boundaries of the Diocese that do not fall under the authority of the Bishop and are not a part of the Diocese. Equally, particular diocesan ministries occur within external institutions (e.g. Prison Chaplaincy, Hospital Chaplaincy).

"Policy" - A statement of purpose or intent for how the Diocese or Agency wants its workers to manage or respond to particular situations. Diocesan policy will support workers understanding of the Diocese's views and values on specific issues, and what will occur if they are not followed. Policies may be imposed or required by external stimuli (civil or canonical law, societal or church regulation) or as a means of promoting or addressing a diocesan priority. A policy can be security related also and that can be used to identify risks and mitigate risks.

"Policy Document" - Codes of Conduct, Governance Policies, Operational Policies and documents such as procedures and guidelines which are subordinate to policy and support the implementation of policy.

"Procedure" - A document that include details about how the policy will be implemented such as who does what, how and when. It should only be as detailed as required to provide adequate guidance to workers to successfully undertake the activity. Procedures that relate to security, risk mitigation or highly technical activities can be lengthy, highly detailed and complex.

"Staff" - All the employees who works at a particular place or in a particular business. It is a subset of the term 'worker'.

"Worker" - A person who carries out work in any capacity for an employer or 'Person Conducting a Business Undertaking'. This includes: • employees; • teachers; • educators; • contractors; • apprentices; • clergy; • religious; • student placements; • trainees; and • volunteers/unpaid . In the Catholic Diocese of Maitland-Newcastle, 'worker' includes those who carry out work in diocesan parishes, within diocesan agencies and as a part of the diocesan curia.

"Clergy" - In Catholic usage, a collective term referring to all those ordained – bishops, priests and deacons – who administer the rites of the church.