

Privacy and Information Protection Policy

1 Purpose and scope

New Meridian University protects information entrusted to it and uses that information for legitimate academic, employment, research, administrative, and safety purposes. This policy explains how student records, personnel information, research data, and complaint materials are collected, accessed, shared, retained, and protected. The President oversees its administration.

This policy applies to students, faculty, staff, research supervisors, contractors, volunteers, and others handling information for NMU. It covers paper and electronic records, messages, recordings, devices, cloud services, and records held by an authorized provider. Responsibilities continue after graduation, employment, a contract, or a university affiliation ends.

NMU does not currently receive federal student aid or other federal financial assistance. This policy establishes institutional student privacy protections without representing the Family Educational Rights and Privacy Act (FERPA) as currently applicable. The President must review legal requirements before changes in funding, university activities, or locations of service. Applicable law, binding agreements, approved research requirements, and specialized NMU procedures remain controlling.

2 Responsibilities and authority

The President approves information protection requirements, designates records custodians and reporting officials, authorizes institutional services, and directs incident response and required notifications. Qualified officials may perform technical assessments and administrative work under the President's authority. Designations and reporting instructions must be communicated when this policy is implemented.

Each custodian maintains an identifiable official record, documents its location and authorized users, checks accuracy, applies retention requirements, and removes access when duties change or an affiliation ends. Research supervisors oversee project data and continuity arrangements. Everyone handling university information must follow approved safeguards, report suspected incidents, and preserve relevant records.

Authority or seniority alone does not justify access to private information. An implicated person or official with a relevant conflict must not control a complaint, its evidence, or its review. Concerns personally implicating the President go to the independent external reviewer designated in advance under NMU's reporting procedures. That reviewer appoints impartial officials to perform the President's case responsibilities; the President does not control or override that review.

3 Collection classification and permitted use

NMU collects information reasonably needed for an identified purpose and explains material uses and disclosures through an appropriate notice, consent document, agreement, or university procedure. Records must be accurate, relevant, and limited to what the activity requires. Users

must not collect additional sensitive information merely because a system permits it, or use information for an unrelated personal, commercial, or discriminatory purpose.

Public information is information authorized for public release. Internal information is operational material intended for authorized university use. Confidential information includes identifiable student and personnel records, research participant information, complaint evidence, financial and identity information, medical or accommodation materials, credentials, and nonpublic contractual information. The custodian assigns protection appropriate to the information and its risks. Uncertainty about classification must be resolved before external disclosure; information is handled confidentially pending that assessment.

Combining records can increase sensitivity or identify a person even when individual fields appear harmless. Names, photographs, enrollment details, contact lists, and research quotations must not be treated as public merely because they are convenient to share. NMU does not sell confidential student, personnel, participant, or complaint information or use it for unrelated advertising.

4 Access storage and secure handling

Access is limited to authorized people who need the information for an assigned responsibility. Custodians approve the appropriate scope, review access periodically, and promptly remove unnecessary permissions. Users must use individual accounts, protect passwords, verify recipients, and avoid shared credentials or unrestricted links. Multifactor authentication must be used for confidential university information where the approved service supports it; an alternative safeguard requires documented assessment and President approval.

Confidential information must be stored and transmitted through approved university arrangements with encryption appropriate to the risk. Personal email, unapproved cloud accounts, public file links, and unsecured removable media must not be used to hold or transfer it. Paper files and devices must be physically protected, screens locked when unattended, and confidential discussions kept from unintended listeners. Remote work requires the same protections.

The President must ensure that approved arrangements include appropriate system updates, access records, secure backups, and recovery procedures. Custodians limit downloads and duplicate copies, preserve essential originals and relevant versions, and verify that records remain accessible throughout their retention period. Technical work must be proportionate to the information involved. A user may not bypass safeguards or expand permissions to complete a task more quickly.

5 Student records

Student records include admissions and enrollment materials, assessment and grade records, academic progress, transcripts, advising records, financial information, accommodations, and disciplinary records maintained for NMU. Instructors, supervisors, and administrators may access only the records needed for their roles. Grades, feedback, identification documents, or a student's circumstances must not be exposed to a class, another student, or an unauthorized recipient.

Students may request access to their own maintained records and correction of inaccurate factual information through the designated custodian or the President. Section 10 explains verification, response periods, restrictions, and review. Parents, spouses, sponsors, employers, and other supporters do not gain automatic access through their relationship to the student or payment of fees. Student authorization or another permitted disclosure basis is required.

Public recognition, photographs, testimonials, and publication of identifiable student information require an appropriate authorization or published procedure establishing the permitted use and any applicable choice to decline. Enrollment or credential verification is handled by the authorized custodian using the minimum information needed. Required permanent academic records preserve an accurate history, including an original award and any authorized subsequent correction or revocation.

6 Personnel information

Personnel information includes applications, appointments, contracts, pay and benefits, evaluations, disciplinary actions, and employment correspondence. Custodians maintain official records securely and restrict access to legitimate hiring, supervision, payroll, benefits, review, or legal needs. A supervisor receives only the information needed to perform an assigned duty.

Medical, disability, and accommodation documentation must be held separately from routine personnel files with more limited access. Supervisors ordinarily receive approved restrictions or adjustments rather than unnecessary medical detail. Complaint and investigation materials are maintained separately; an authorized final employment action may be recorded in the personnel file as necessary.

Faculty and staff may request access to their own maintained personnel records, correction of factual errors, and inclusion of a relevant written response to a disputed evaluation or document. Appropriate restrictions protect another person's information, confidential references, legally privileged material, and a fair ongoing review. Employment verification and reference requests must follow the authorized disclosure procedure.

7 Research data and participant confidentiality

Before collecting or receiving research data, the supervisor or project lead must document the data to be collected, permitted uses, responsible custodian, storage, access, sharing, retention, and disposal. The plan must satisfy applicable consent commitments, approved research requirements, licenses, and agreements. Researchers must explain relevant confidentiality limits to participants and obtain required permissions before recording, collecting sensitive information, or changing an approved use.

Identifiable participant information must be limited to what the project requires. Coding keys must be stored separately with restricted access. Removing names or assigning codes does not establish anonymity: quotations, images, combinations of characteristics, and linked datasets can permit identification. Publication and data sharing require assessment of identification risk and any necessary consent or agreement. Participant information must not be placed in an open repository merely to support reproducibility.

Data needed to support findings include relevant source records, consent documentation, methods, code, metadata, and correction histories. Research records are ordinarily retained for seven years after project completion or publication, whichever is later, as required by the Academic Integrity and Research Misconduct policy. The integrity officer documents reconciliation with different applicable retention or destruction requirements and approved consent or data-management terms, including whether nonidentifiable documentation can be retained. Preservation obligations remain controlling; identifiable information is retained only as authorized and necessary.

A departing researcher must arrange authorized custody and continued access needed for research verification and unfinished student work. Transfers or retained copies require approval, secure handling, and compliance with applicable agreements and participant permissions. This policy establishes stewardship responsibilities without assigning ownership of all student work or changing authorship and intellectual property rights.

8 Complaint materials and fair process

The Office of Ethical Compliance and authorized case officials maintain complaint reports, evidence, correspondence, protective measures, findings, decisions, appeals, and implementation records securely. Access is limited to legitimate safety, administration, investigation, response, appeal, implementation, or legal needs. Case materials must not circulate as gossip or be disclosed to expose a participant to hostility.

Confidentiality cannot be guaranteed in every case. Relevant information may need to be shared to investigate an allegation, provide a fair response, implement protection, or meet a legal requirement. Officials must explain material confidentiality limits. Anonymous information may be considered, but identity may be apparent from the facts and anonymity can limit the available response. Confidential or legally privileged status must not be promised unless that protection actually applies.

Parties retain the notice, relevant evidence, response, hearing, and appeal rights provided by the governing NMU procedure. Unrelated private information may be redacted or protected by another fair method while preserving a meaningful opportunity to respond to evidence used in the decision. A reporter or witness who is not a party ordinarily receives an appropriate completion notice and information about that person's own safety or access, rather than another person's full case file or private disciplinary outcome.

Participants may obtain advice, support, relevant evidence, and outside assistance. Privacy instructions must not prevent protected reporting or participation. A person may not use access to case materials to intimidate others, interfere with evidence, or retaliate. Receiving a record for a case does not authorize unrelated publication or reuse of another person's private information.

9 Outside disclosures providers and technology

External disclosure of confidential records requires informed authorization from the person concerned or a documented permitted basis, such as an approved service arrangement, necessary research agreement, valid legal requirement, authorized case procedure, or a necessary response to a serious safety threat. Authorization must identify the information, recipient, purpose, and

scope. Revocation applies to future consent-based disclosure, subject to controlling requirements; it does not reverse a completed authorized disclosure.

The custodian verifies the recipient, confirms the authority to release the information, limits the disclosure, and records its basis and date. Subpoenas, court orders, law enforcement requests, and requests involving uncertainty go promptly to the President for legal assessment and timely response. Urgent safety disclosures must be limited and documented. Required research notifications follow the Academic Integrity and Research Misconduct policy. An outside requester does not acquire access simply by asserting authority.

Before a provider receives confidential information, the President approves the arrangement after appropriate privacy and security assessment. Written terms must address permitted use, access, safeguards, subcontractors, retention, return or secure disposal, and prompt incident reporting and cooperation. Transfers across jurisdictions require review of applicable restrictions. A provider may use university information only for the authorized purpose and may not independently sell it, advertise with it, or reuse it for model training.

Confidential information must not be entered into public or personal AI services. Any AI use involving confidential information requires the President's written approval of the specific service, account or institutional workspace, purpose, and information category under the Artificial Intelligence and Technology Use policy. General academic permission, a subscription, a privacy setting, consent alone, or removal of names does not establish that approval. Connected tools, recordings, transcription, and meeting assistants require appropriate approval, notice, necessary consent, and compliance with applicable research requirements before use.

10 Requests for access correction and explanation

A request should identify the record sought, the requested access or correction, and a way to respond. The custodian verifies identity and any representative's authority using a proportionate method. Requests must not require unnecessary sensitive information. NMU acknowledges a request within five business days and ordinarily provides access, a correction decision, or a reasoned response within thirty calendar days after receipt. A controlling shorter deadline applies. Any necessary extension must be explained before the response period ends with an updated date; it cannot defeat an applicable legal right.

Access may be provided through secure copies, supervised inspection, or another practical arrangement. Restrictions or redactions must have a specific reason, including another person's privacy, applicable privilege or law, or a necessary and proportionate protection for an ongoing review. A case participant's relevant evidence rights remain controlling. The response explains a full or partial refusal and the available review route. NMU must not destroy a requested record while the request or its timely review is pending.

Verified factual errors must be corrected with an appropriate record of the change. A person may provide a relevant written statement when a factual correction is denied or a professional evaluation is disputed. Access and correction requests do not replace grade review, authorship review, or misconduct appeals and do not erase accurate required records. Concerns about refusal, redaction, delay, or handling may be reported under the Reporting Ethical Concerns and

Complaint Procedures policy, with its impartial decision and independent appeal safeguards. This policy creates no additional appeal of a final specialized decision.

11 Retention preservation and secure disposal

The President approves written retention schedules for student, personnel, and administrative records. Each schedule identifies the official custodian, record category, required period, starting event, and authorized disposition. Retention must reflect applicable requirements and a documented continuing need. Routine deletion must not occur before the applicable schedule is established and required checks are completed.

Complaint records are ordinarily retained for at least seven years after final resolution. Specialized longer or permanent requirements remain controlling, including permanent final records of expulsion, invalidated credit, degree revocation, or termination required by the Academic Integrity and Research Misconduct policy. Research retention follows Section 7. Official transcript and credential history must be preserved permanently, subject to applicable requirements.

A pending or reasonably anticipated complaint, investigation, appeal, access request, audit, legal proceeding, or preservation instruction suspends relevant routine destruction. Custodians preserve originals, material versions, access records, and relevant messages as appropriate. A hold is released only by the authorized official after applicable obligations are assessed. No one may delete or alter records to conceal an incident or allegation.

When authorized retention ends and no hold applies, records must be securely destroyed or rendered indecipherable. Disposal includes paper, devices, removable media, duplicate files, and provider-held copies as applicable. Backup copies remain protected and expire under documented backup procedures; they must not become uncontrolled archives. The custodian documents disposal of confidential official records and verifies provider return or disposal when an arrangement ends.

12 Incidents complaints and continuing review

A suspected loss, unauthorized access, mistaken disclosure, compromised account, unsafe AI upload, or improper alteration must be reported immediately upon discovery to the President or designated official. Proof of harm is not required before reporting. Stop affected use where feasible, preserve relevant evidence securely, and follow containment instructions. Do not forward exposed records unnecessarily or delete evidence while attempting to correct the incident. President-related concerns follow the independent external route in Section 2.

The President directs prompt assessment, qualified containment and recovery, identification of affected records and people, and any required notices to individuals, data owners, providers, or authorities. The response must assess the applicable jurisdictions, legal definitions, notification triggers, deadlines, and contractual duties. Required notices must not await completion of a disciplinary case. The incident record documents the known facts, protective steps, notification decisions and reasons, and corrective follow up.

Utah's Protection of Personal Information Act requires reasonable safeguards and secure destruction for covered personal information, and prompt investigation of a qualifying system breach. Where the statutory conditions apply, NMU must notify affected Utah residents, notify the Attorney General and Utah Cyber Center at the threshold of 500 affected Utah residents, and notify nationwide consumer reporting agencies at the threshold of 1,000 affected Utah residents. Required notices must be made expeditiously without unreasonable delay under the applicable law. Other jurisdictions or agreements may require additional or earlier action.

Suspected policy violations follow the Reporting Ethical Concerns and Complaint Procedures policy unless a specialized NMU process or controlling requirement applies. Academic and research misconduct retains its own findings, sanction, and appeal authority. Corrective or disciplinary action must follow the applicable notice, response, hearing, and independent appeal protections, including serious-sanction safeguards. Good-faith reporting and participation are protected under the Protection from Retaliation policy.

The President reviews implementation periodically, provides appropriate instruction to information users, and checks that custodians, approved services, reporting arrangements, retention schedules, and incident procedures remain suitable. Material changes are communicated through university channels. Individuals may seek outside assistance without first exhausting NMU's process; internal review does not extend an external filing deadline.

Approval date October 1, 2026

Effective date October 1, 2026

Billy Whisnant, Ph.D., President