



POLICY NAME	Acceptable Use of Licensed Resources	POLICY NO.	BA468
APPROVING BODY	President/Cabinet	VERSION NO.	01
RESPONSIBLE DEPARTMENT	Business Affairs- Information Technology		
EFFECTIVE DATE	Date	REVIEW/REVISION DATE	NEW

PURPOSE:

The purpose of this policy is to establish the acceptable use of University provided Licensed Resources at Western New Mexico University (WNMU). Licensed Resources are provided to support the University's educational, research, administrative, and public service missions. This policy ensures these resources are used responsibly, ethically, securely, and in compliance with applicable laws, licensing agreements, and University policies.

This policy applies to all current and future licensed software, cloud services, subscriptions, and technology resources provided or managed by the University unless superseded by a service specific policy or licensing agreement.

POLICY:

The Acceptable Use Policy for Licensed Resources establishes the requirements for the responsible, ethical, secure, and lawful use of University-provided Licensed Resources. This policy applies to all faculty, staff, students, emeritus recipients, and other authorized users. Licensed Resources include, but are not limited to, Microsoft 365 applications and services (such as Outlook, Word, Excel, PowerPoint, OneDrive, SharePoint, and Teams), Adobe Creative Cloud, and any other software, cloud service, subscription, or technology resource licensed by the University.

Acceptable use supports the University's educational, research, administrative, and public service missions. Prohibited activities include unauthorized access, distribution of malicious software, misuse of University data, and any activity that violates University policy or applicable law.

Eligibility for Licensed Resources is determined by University affiliation and employment or enrollment status as described in Section 6, Access and Account Management.

Users are responsible for protecting their accounts through strong passwords or passphrases, multi-factor authentication where required, and compliance with all applicable University information technology policies.

SCOPE:

This policy applies to all WNMU faculty, staff, students, emeritus recipients, contractors, affiliates, and other authorized users who access or use University-provided Licensed Resources.

Licensed Resources include, but are not limited to:

- Microsoft 365 applications and cloud services
- Adobe Creative Cloud
- University-licensed desktop software
- Software-as-a-Service (SaaS) platforms
- Cloud storage services
- Collaboration platforms
- Artificial intelligence services
- Any current or future software, application, subscription, or technology resource licensed or managed by WNMU

This policy applies unless superseded by a more specific University policy or software licensing agreement.

TERMS:

Licensed Resources: Software, cloud services, applications, subscriptions, and other technology resources licensed, subscribed to, or otherwise provided by Western New Mexico University for academic, research, administrative, or institutional purposes. Examples include, but are not limited to, Microsoft 365, Adobe Creative Cloud, Teams, OneDrive, SharePoint, and future licensed services.

Users: All WNMU faculty, staff, students, emeritus recipients, contractors, affiliates, and other authorized individuals who have been granted access to Licensed Resources.

ACCEPTABLE USE:

Users are expected to use Licensed Resources in a manner consistent with WNMU mission and vision.

Acceptable use includes, but is not limited to:

- **Academic and Administrative Use:** Using Licensed Resources for instruction, coursework, research, administrative operations, communication, and other official University activities.
- **Collaboration:** Using Licensed Resources to collaborate with University personnel, students, external partners, and other approved organizations when such collaboration complies with University policies and applicable licensing agreements.
- **Communication:** Using Licensed Resources for professional and academic communication in support of University business.
- **Authorized Business Operations:** Using Licensed Resources to perform responsibilities associated with employment, enrollment, or other authorized University activities.

UNACCEPTABLE USE:

Users must not engage in activities that compromise the integrity, security, availability, or lawful use of University systems, data, or Licensed Resources.

Prohibited activities include, but are not limited to:

- **Unauthorized Access:** Attempting to access accounts, systems, applications, or information for which the user is not authorized.
- **Malicious Activity:** Introducing, transmitting, distributing, or executing malware, ransomware, viruses, malicious code, or other harmful content.
- **Data Misuse:** Accessing, sharing, storing, or distributing confidential, proprietary, or sensitive University information without proper authorization.
- **License Misuse:** Installing, copying, sharing, transferring, or using Licensed Resources in violation of University licensing agreements or vendor licensing terms.
- **Personal Commercial Activity:** Using Licensed Resources primarily for personal commercial purposes, private business activities, political campaigning, or other non-University purposes unless expressly authorized.
- **Illegal or Prohibited Activities:** Engaging in activities that violate University policies or local, state, federal, tribal, or international laws or regulations.
- **Email Forwarding:** Automatic forwarding of University email to external email accounts is prohibited unless specifically approved by Information Technology. Unauthorized forwarding rules may be removed without prior notice to protect University information.
- **Personal Use:** Limited personal use of Licensed Resources may be permitted provided it does not interfere with University operations, violate licensing agreements, consume excessive resources, or conflict with University policy. Users should understand that communications and records maintained within University systems may be subject to disclosure under the New Mexico Inspection of Public Records Act (IPRA) or other applicable laws.

ACCESS AND ACCOUNT MANAGEMENT:

- **Current Students:** Students currently enrolled at WNMU are eligible for Licensed Resources appropriate to their academic status.
- **Graduates and Non-Enrolled Students:** Graduates and students who are no longer enrolled may retain access to designated Licensed Resources for up to 365 days following the end of their last enrolled term. After this period, accounts may be disabled and licenses removed.
- **Current Employees:** Current full-time and part-time employees are eligible for Licensed Resources appropriate to their employment responsibilities.
- **Terminated, Resigned, or Deceased Employees:** Access to Licensed Resources will remain active until the employee's separation date or notification from Human Resources. Upon notification, access may be suspended immediately and licenses removed in accordance with University procedures.

- **Adjunct Employees:** Adjunct employees are eligible for Licensed Resources while under an active employment contract. Access may be disabled following the census date of the second consecutive semester in which no active contract exists.
- **Emeritus Employees:** Individuals granted Emeritus status by approval of the University President and/or the Board of Regents may retain access to designated Licensed Resources as determined by the University. Existing employee accounts may be replaced with emeritus-designated accounts when appropriate. Emeritus accounts that remain inactive for twelve consecutive months may have associated licenses removed following advance notification from Information Technology.

SECURITY AND PRIVACY:

- **Account Security:** Users are responsible for protecting their accounts through strong passwords or passphrases and must not share login credentials.
- **Multi-Factor Authentication:** Users must utilize multi-factor authentication where required by University policy or technical controls.
- **Compliance:** Users must comply with all other applicable University policies governing information security, data protection, privacy, records retention, and acceptable use.
- **Privacy:** While the University respects user privacy, users should not expect complete privacy when using University-owned systems. The University reserves the right to access, monitor, audit, and preserve information contained within Licensed Resources as permitted by law and University policy.

DATA MANAGEMENT:

- **Storage Limits:** Users must comply with storage limits established by Information Technology. Current default storage allocations may be modified as licensing agreements, operational requirements, or institutional needs change.
- **Data Management:** Users are responsible for maintaining and organizing their University data and should periodically perform file maintenance to ensure efficient use of storage resources. Users should follow all University and State of New Mexico Records Retention policies.
- **Backup and Recovery:** Users are responsible for ensuring that locally stored University data is appropriately backed up. Data stored within University-managed cloud services is subject to the University's backup, retention, and recovery capabilities, which do not replace a user's responsibility to protect critical information.

ENFORCEMENT:

- **Monitoring and Auditing:** The University reserves the right to monitor, audit, and review the use of Licensed Resources as permitted by applicable law, licensing agreements, and University policy to ensure compliance and protect University systems.
- **Violations:** Violations of this policy may result in suspension or revocation of access to Licensed Resources, disciplinary action under applicable University policies, financial liability for licensing violations where appropriate, and referral for civil or criminal action when warranted.

- Information Technology may immediately suspend access to Licensed Resources when necessary to protect University systems, data, users, or licensing compliance.

DOCUMENT CONTROL REGISTER*				
For Internal Use Only – Master Document				
DOCUMENT TITLE:		DOCUMENT NO.	EFFECTIVE DATE:	
Acceptable Use of Licensed Resources Policy		BA468		
DOCUMENT LOCATION: (Where is this document referenced or located; include links to SharePoint or any other locations that are accessible)				
REVIEW HISTORY (Complete log for review only)				
REVIEWED	REVIEW DATE:		REVIEWED BY:	
<u>ANNUAL REVIEW</u>	<u>16-OCT-2026</u>		<u>Michael Acosta</u>	
REVISION HISTORY				
(For audit purposes and control tracking)				
REASON FOR REVISION: **	REVISED SECTION, PAGE#, and PARAGRAPH:	VERSION #:	REVISION DATE:	APPROVED BY:
NEW POLICY	NEW	01	16-OCT-2026	VPBA