# UNMLA Acceptable Computer Use Policy:

The University of New Mexico at Los Alamos provides access to computers for purposes of education, research, and student service. Academic purposes may include operations fulfilling classroom assignments, academic discovery, career development, instructional support, and other goals related to university directed activities. Use of computers for purpose outside these guidelines is not provided or encouraged. Unless otherwise stated all UNMLA IT policies mirror the UNM IT Acceptable Use Policy. **In any case where local UNMLA policy may be unclear, conflicting, or not explicitly stated it is the UNM IT Acceptable Use Policy that will be followed as practicable.**

**Please note that UNMLA IT admins may access or be granted access to all data on UNMLA owned computers, including browser cache, document folders, picture folders, logs, etc. as a function of their roles. Any illegal materials found on a device during direct or incidental searches will be reported.**

**The UNMLA IT Acceptable Computer Use Policy document is subject to change without notice.**

## Effective Dates:

The following UNMLA IT policies are considered current and in effect as of 7/19/2023.

## UNMLA IT Contact Information:

A UNMLA IT ticket may be made by any faculty or staff member using the Asset Essentials login.

DeBray Bailey: baileyd@unm.edu

Hours: 9AM – 6PM

Teams: baileyd

Neil Stoddard: nstoddard@unm.edu

Hours 7:30 AM – 4:15PM

Teams: nstoddard

UNMLA IT is located underneath building 2 in rooms 113 and 113A. If we are not in our offices please create a ticket or use Teams (or email) to contact us.

# UNMLA Computer Accounts, User Identification, and Access Control

**Computer Access Control:**

Computer labs are open during regular hours of operation and may be used by any enrolled student provided that the room is not in use by an instructor. Computer lobby areas are open during UNMLA's regular hours of operation and may be used as available. When campus closes, all computer labs become inaccessible. Servers for courses using Linux along with website resources such as the UNMLA website and UNM's Canvas online courses will still be available online.

**Computer Login for Students:**

UNMLA Students who wish to use the computer labs or other classroom equipment on campus must have a valid UNM NetID login or be currently enrolled in a continuing education or GED related course. Selected laboratories in "hands on" lab classrooms may use a generic login with close instructional supervision due to the nature of the work done in the course (example: PPE is being worn).

**Computer Login for Guests:**

UNMLA guest speakers and instructors may use select computer lectern equipment without a NetID login. That equipment is located in lecture halls: Wallace Hall, 631, and 230. For guests requiring access to equipment in other areas please make that request ahead of time via your contact at UNMLA Facilities & Rentals, or the Administrative Assistant at the Dean of Instruction.

**Computer Login for Faculty and Staff**:

Faculty and Staff must use the standard UNM NetID and password to log into classroom and office computers. If your UNM NetID is not working please call UNM IT for a password reset at: 505-277-5757 between the hours of 7:30AM-5PM M-Fr. You may also use the "Forgot UNM NetID password" selection at the UNM NetID Page. If you need immediate assistance please contact Neil or DeBray on campus (extension 339 or 405).

# UNMLA Printers:

**Students:**

UNMLA IT asks that printing be kept to the minimum amount necessary as required by your instructor. This policy is in cooperation with UNM sustainability guidelines. Please note that the printing of textbooks is **explicitly disallowed** and attempting to do so may result in **revocation of printing privileges** and/or other academic disciplinary measures.

There are black and white laser printers in every computer lab classroom. Lobbies of building 6 and 3 also have printers available. A color laser is available for use by students in the Academic Support Center in building 2.

In addition to the standard printers, a large format Epson printer is also provided to students in the Mac Lab, but we ask that an appointment be made with IT (or your instructor) before use of that specific printer.

If a classroom or lobby printer has run out of toner or paper please inform UNMLA IT or your instructor.

**Faculty and Staff:**

UNMLA IT asks that printing be kept to the minimum amount necessary as required by your course. This policy is in cooperation with UNM sustainability guidelines.

Xerox copier / scanner machines are provided in buildings 2 (basement), 6 (lounge), and 1 (Student Services) and require a copy code to operate for most printing tasks. Copy codes are provided by UNMLA IT (staff) or Instruction (Faculty).

# UNMLA Network and WIFI:

Please note: The UNMLA network is governed by the UNM IT Acceptable Use Policy.

**WIFI Policy:**

UNMLA provides WIFI access to all students and patrons using one of three available networks:

"**Lobo-Guest**" is open to all guests of UNMLA as a non-secured WIFI connection. The Acceptable Use Policy popup must be agreed to when signing in.

"**Lobo-wifi**" is open to all students, faculty, and staff. The sign-in is the standard UNM NetID and password.

"**eduroam**" is intended for visiting faculty and staff. It can be logged into using most New Mexico college sign-in credentials (whatever the UNM NetID / password equivalent might be).

## UNMLA Downtime, Unexpected Maintenance, and Data Loss:

While all efforts are made to keep computer equipment and networks operational UNMLA Computer downtime and unexpected maintenance may occur without warning. UNMLA IT is not responsible for data loss incurred by power outage, equipment failure, 3rd party data hosting, human error, or natural disaster where users have chosen to not sync their files to OneDrive or SharePoint.

**Students:**

UNMLA Student users are **highly encouraged** to save their data to UNMLA provided storage and use the UNM provided OneDrive service to sync their files. Files saved outside of UNM provided cloud services may not be recoverable!

**Faculty and Staff:**

UNMLA employees are **highly encouraged** to save their data to UNMLA provided storage (SharePoint) and use the UNM provided OneDrive service to sync their files. Any data saved to a removable device that could easily be lost or stolen should be **encrypted**. Files saved outside of UNM provided cloud services may not be recoverable!

## UNMLA Cybersecurity and Incident Response:

**Students:**

Students attending the standard UNMLA New Student Orientation will receive a short cybersecurity briefing that includes information on what to do in case of virus, ransomware, or other malware.

**In case of a student laptop viral infection** the laptop should be returned for UNMLA for cleaning and UNMLA IT should be notified immediately.

**In case of a UNMLA desktop viral infection** Unplug the desktop machine from the network (blue or gray cable) and notify UNMLA IT immediately. Do not turn the machine off as data may be lost.

**In case of email phishing scam or ransomware activation** the user's UNM NetID password should be changed, the laptop should be returned, and the UNM Report Phishing Site should be notified immediately (along with UNMLA IT).

In both cases a fresh laptop can be issued once the virus/malware incident is secure and another brief cybersecurity tutorial has been given.

**Faculty and Staff:**

Faculty and Staff are encouraged to attend one of several IT Cybersecurity Orientations that will be (tentatively) held starting Fall of 2023. Until local live sessions are available, faculty and staff are encouraged to review UNM IT cybersecurity's Awareness Page.

**In case of a laptop viral infection** the laptop should be returned for UNMLA for cleaning and UNMLA IT should be notified immediately.

**In case of a desktop viral infection** Unplug the desktop machine from the network (blue or gray cable) and notify UNMLA IT immediately. Do not turn the machine off as data may be lost.

**In case of email phishing scam or ransomware activation** the user's UNM NetID password should be changed, the laptop should be returned, and UNMLA IT should be notified immediately.

In both cases a fresh laptop can be issued once the virus/malware incident is secure and another brief cybersecurity tutorial has been given.

In cases where an active breach of security has happened where a large quantity of data is known to be lost to an outside hacker, UNM IT will be notified and all policies involving cybersecurity will be followed at the Main Campus IT level. Where security breaches are confined to a single PC on campus, or are not serious (example: malware that merely shows users advertisements), the incident can be remedied inside UNMLA IT. **If there is doubt about an infection, email, or file, please contact UNMLA IT.**

## UNMLA Computer Laptop Checkout and Tracking:

**UNMLA reserves the right to use and install equipment tracking software, remote login software, and/or soft lock-out software to help maintain its inventory. This category of software may provide UNMLA IT with user location information, access to all user files, etc. Users checking out UNMLA IT equipment implicitly agree to these policies and conditions on checkout of equipment.**

**Students:**

Currently enrolled students of UNMLA may check out a laptop for academic use through the UNMLA Learning Resource Center.

Laptops may be checked out to students at any time during a full semester (spring, summer, or fall) but they must **always** be returned by the end of finals week of that same semester. Laptops may be checked out again at the start of the following semester.

Students may receive a different laptop each checkout period and no expectation of data preservation can be assumed as all laptops are subject to a data wipe process. Students are encouraged to use OneDrive to save their data.

Laptops must be connected to the UNM network approximately every 6 months to reactivate software. Generally, this occurs automatically upon logging into Lobo WIFI or plugging into the hard-wired UNMLA network. In cases where the software fails to activate itself the laptop can be brought by UNMLA IT for activation during normal working hours. Students are encouraged to turn on their laptops at the time of checkout to make sure that the unit they have received has activated software.

Students who do not return their laptops will have their accounts flagged and may not be able to enroll for another semester until the equipment is returned or other arrangements are made. **Laptops not returned within 5 business days of the due date may be reported as stolen by UNMLA IT**. **Alternatively, a hold may be placed on your account until all UNMLA equipment has been returned.**

**Acceptable return methods include**: physical return to the UNMLA library (IE: directly handed to a UNMLA librarian).

**Unacceptable return methods include, but are not limited to**: dropping off laptops in the return bin, putting laptops outside a door, giving the laptop to a non-Learning Resource Center personnel, returning the laptop to a different campus, returning the laptop without all equipment (missing power adapter, etc.).

Students who return laptops that have been obviously abused may receive disciplinary action, repair fees, and/or have their laptop checkout privilege revoked.

**Faculty and Staff:**

Currently employed staff and routinely returning faculty may checkout a laptop for work use through the UNMLA Learning Resource Center. The checkout period is until the life expectancy of the laptop is reached or until cessation of employment.

Laptops must be connected to the UNM network approximately every 6 months to reactivate software. Generally, this occurs automatically upon logging into Lobo WIFI or plugging into the hard-wired UNMLA network. In cases where the software fails to activate itself the laptop can be brought by UNMLA IT for activation during normal working hours. Users are encouraged to turn on their laptops at the time of checkout to make sure that the unit they have received has activated software.

**Laptops and other IT equipment not returned within 24 hours of the end of employment may be reported as stolen by UNMLA IT.**

**Acceptable return methods for IT equipment include**: physical return to the UNMLA Learning Resource Center (IE: directly handed to a UNMLA librarian), physical return to UNMLA IT (IE: directly handed to UNMLA IT personnel). If an employee is **out of state** a laptop may be returned via a well packaged, insured, tracked, and UNMLA approved shipping carrier method (IE: UPS, USPS, or FedEx). In some cases, this may be at the employee's expense. A tracking number must be provided to UNMLA IT at the time of shipment.

**Unacceptable return methods for IT equipment include but are not limited to**: dropping off laptops in the return bin, putting laptops outside a door, giving the laptop to a non-Learning Resource Center or UNMLA IT personnel, returning the laptop to a different campus, returning the laptop without all equipment (missing power adapter, etc.).

Staff or Faculty who return laptops that have been obviously abused may have their laptop checkout privilege revoked.

All laptops issued to UNMLA Faculty or Staff must have BitLocker (or equivalent) encryption activated. Purposefully disabling BitLocker (or equivalent) encryption will result in loss of laptop checkout privilege and possibly other disciplinary measures.

## UNMLA Software Purchase:

All UNMLA software and web service purchases begin with an Asset Essentials ticket to UNMLA IT. The software is evaluated for compatibility with our on-campus systems first and then must pass the Purchasing Risk Assessment from Main Campus IT.

All university software procurement requests are reviewed by appropriate UNM personnel who verify that the vendors in question meet the contractual and regulatory obligations UNM has for handling sensitive information. The following type of information is reviewed (this list is not all-inclusive and other data may be evaluated as needed):

- Banner ID (FERPA/HIPAA Identifier).
- Credit Card Information (regulated by the Payment Card Industry).
- Direct Deposit information (regulated by Federal Trade Commission).
- Institutional Review Board (IRB) activities.
- Protected Health Information (PHI) (regulated by Health Insurance Portability and Accountability Act – HIPAA).
- Social Security Number (SSN) (regulated by Federal Privacy Act of 1974).
- Student Grades and other academic records (regulated by Family Educational Rights and Privacy Act – FERPA).
- Student Loan information (regulated by Gramm Leach Bliley Act - GLBA)

For more information on this process, please see the UNM Purchasing Risk Assessment Website.

## UNMLA (low-cost multi-function) Printer Purchase:

Large multi-function printers are provided to UNMLA personnel in buildings 1, 6, and 2 (downstairs). Scanning is free of charge, but printing requires a UNMLA copy code. A copy code may be requested by a departmental assistant or supervisor using a request in Asset Essentials.

In the spirit of cost effectiveness and helping to meet UNM environmental goals, the purchase of low-cost multi-function printers is **discouraged,** but not impossible. To purchase such a device please read the UNM Print Management MFD Approval Request and sign the acknowledgement, then attach the acknowledge document to the your UNMLA Asset Essentials IPR.

## Misc.:

All IT Policies not explicitly listed this UNMLA IT policy document (legal, security, misuse, privacy, etc.) will mirror those found at the UNM IT Acceptable Use Policy where practicable.