Microsoft 365 for Education offers convenient cloud-based services to facilitate your work at University of Louisiana at Lafayette (UL Lafayette). Microsoft 365 for Education (Microsoft 365) includes OneDrive, a cloud file storage and sharing service, as well as other online applications that may be made available to you. Although Microsoft 365 is a University-licensed cloud solution, there are security practices that must be followed to ensure the service is used in a manner that best protects the security of the University's confidential and sensitive data.

This agreement provides rules regarding the acceptable use of Microsoft 365 by members of the UL Lafayette community for university academic, research and administrative purposes. These rules are applicable only to Microsoft 365 and not to other cloud-based applications and services and supplement UL Lafayette's general Acceptable Use of Computer Resources policy. If you have any questions, please check with the data owner or the UL Lafayette CIO.

I. Benefits of Microsoft 365

- Microsoft 365 is UL Lafayette-licensed for use by the University and supported by UL Lafayette IT and college IT departments.
- Microsoft 365 / OneDrive offers generous file storage. OneDrive can automatically synchronize files across platforms and devices, e.g., PC, Mac, and mobile devices.
- Microsoft 365 facilitates file sharing and collaboration among UL Lafayette students, faculty and staff in accordance with the classifications of data described in the sections that follow.
- Microsoft 365 / OneDrive facilitates the sharing of public files (see Section VI *Sharing Public Data*) with colleagues both inside and outside of the University.

II. Using Microsoft 365 Securely

You as the User are responsible for securing every workstation or device you are using to access Microsoft 365 services. Talk to your college or the IT Service Desk to get help or answers to questions regarding securing your computers and other devices.

- Ensure virus/malware detection software is installed with the latest definitions.
- Keep your operating system and software up-to-date.
- Password-protect your workstation or device and use idle-time screen saver passwords where possible.
- Only use your workstation or device with the privileges of a regular user—not as a system administrator.
- Take particular care to maintain these precautions when using OneDrive to synchronize files to a device that is not issued and managed by the University.

III. Protecting Your Data in Microsoft 365

You as the User are also responsible for protecting the data you choose to store in Microsoft 365.

- Periodically review security and sharing settings, ensuring that information is shared only with intended audiences.
- Back up any valuable data you store in Microsoft 365 so that Microsoft 365 is not the sole repository of the data.
- Files must be stored in accordance with University and college records retention schedules.
- Storing personal files or information in your UL Lafayette Microsoft 365 account is not recommended. Data present in your UL Lafayette Microsoft 365 account may be subject to open records requests.

IV. Protecting Confidential Data

Confidential data includes data that, if accessed by unauthorized entities, could cause personal or institutional financial and reputational loss or constitute a violation of a statute, act, law or University policy.

Confidential information should not be stored in Microsoft 365 unless the specific use has been reviewed and approved by the University's IT Security Officer (ITSO) in consultation with relevant offices possessing expertise on the type of data involved, including the Provost.

Examples of confidential data include but are not limited to:

- Personally Identifiable Information (PII) including but not limited to social security number, date of birth, mother's maiden name, passport number, driver's license number, taxpayer identification number, bank account and credit/debit card numbers.
- Data, such as student educational records, covered by the Federal Educational Rights and Privacy Act (FERPA). This includes class rosters, test scores, grades and financial aid information that can be associated with an individual.
- Protected Health Information (PHI), including medical records, health status, and records covered by health privacy laws.
- Citizenship information.
- Payment cardholder information requiring protection under the Payment Card Industry Data Security Standard (PCI DSS), such as credit and debit card numbers, card expiration, etc.
- Trade secrets, intellectual property or information that may be relevant for the creation of a University, faculty or student owned patent.
- Research data under a restricted data use agreement or other IRB data and relevant restrictions that do not explicitly permit cloud storage.
- Passwords and access codes.

V. Protecting Sensitive Data

Sensitive data is information generally used internally at the University or with its authorized partners. If released to unauthorized individuals, sensitive data would not result in financial loss or legal compliance issues but would negatively affect the privacy of the individuals named or the integrity or reputation of the University.

Sensitive data may be stored and shared in Microsoft 365 but must be stored and shared in a secure manner in accordance with Sections II and III above regarding "Using Microsoft 365 Securely" and "Protecting Your Data in Microsoft 365"

This includes but is not limited to the following:

- Email and other communications regarding internal matters which have not been specifically approved for public release.
- Proprietary financial, budgetary or personnel information not explicitly approved by authorized parties for public release.
- Identities of donors or other third-party partner information maintained by the University not specifically designated for public release.

VI. Sharing Public Data

Public Data refers to data that does not meet the criteria for Confidential or Sensitive Data as defined above. Although not Confidential or Sensitive, to maintain its integrity access to Public Data must be managed in a safe and secure manner.

Public data may be stored and shared in Microsoft 365.

Best practices for sharing Public Data:

- Use folders to share groups of files with others online.
- Share files with specific individuals, never with "everyone" or the "public."
- Be careful when sending links to shared folders because they can be forwarded to others to whom you did not intend to provide access.
- Remember that once a file or information is shared, the recipient can download it to a device and share it with others.
- Remove individuals when they no longer require access to files or folders.
- Shared OneDrive files and folders will have a defined time limit on their sharing. That time limit can be renewed.

APPLICABLE UL LAFAYETTE IT POLICIES:

- Comprehensive Information Security Program: *http://helpdesk.louisiana.edu/sites/helpdesk/files/UL%20Lafayette%20Comprehensive%20Information%20Security%20Program%20-%202014.pdf*

RELATED UL LAFAYETTE IT STANDARDS:

- UL Data Classification Policy: *http://helpdesk.louisiana.edu/sites/helpdesk/files/Data%20Classification%281%29.pdf*
- Data Handling for Guidelines for Microsoft Office 365: *https://it.louisiana.edu/sites/it/files/Data%20Handling%20Guidelines%20for%20Microsoft%20Office%20365%20at%20UL%20Lafayette.pdf*

RESPONSIBLE OFFICE: Information Technology

APPROVAL AUTHORITY: Gene Fields, Chief Information Officer

STANDARD EFFECTIVE DATE: 4 September 2024

NEXT SCHEDULED STANDARD REVIEW: July 2025

STANDARD REVISION HISTORY:

Date	**Change Description**
1 July 2024	Matt Delcambre: Initial draft submitted
4 September 2024	Approved by Gene Fields