Acceptable Use of Microsoft Office 365 for Education Policy

Microsoft Office 365 for Education offers convenient cloud-based services to facilitate your work at CUNY. Office 365 for Education (Office 365) includes OneDrive for Business, a cloud file storage and sharing service, as well as other online applications that may be made available to you. Although Office 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 policy provides rules regarding the acceptable use of Office 365 by members of the CUNY community for CUNY academic, research and administrative purposes. These rules are applicable only to Office 365 and not to other cloud-based applications and services and supplement CUNY's general Acceptable Use of Computer Resources policy. If you have any questions, please check with the data owner, the college CIO or CUNY CIS in the Central Office.

I. Benefits of Office 365

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

II. Using Office 365 Securely

You as the User are responsible for securing every workstation or device you are using to access Office 365 services. Talk to your college or Central Office IT department 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 Office 365

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

- Periodically review security and sharing settings, ensuring that information is shared only with intended audiences.
- Back up any valuable data you store in Office 365 so that Office 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 CUNY Office 365 account is not recommended. Data present in your CUNY Office 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 Office 365 unless the specific use has been reviewed and approved by the University's Chief Information Security Officer (CISO) or the college Chief Information Officer (CIO), 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 Office 365 but must be stored and shared in a secure manner in accordance with Sections II and III above regarding "Using Office 365 Securely" and "Protecting Your Data in Office 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 Office 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.

Related information:

CUNY Acceptable Use of Computer Resources Policy

CUNY Information Security Procedures

Acceptable Use of Microsoft Office 365 for Education	**Issue Date:** 7/23/2018
	Issued By: University Cloud Policy Advisory Group **Policy Owner:** Computing and Information Services