Acceptable Use Guidelines for OneDrive

Mercy College offers faculty and staff OneDrive for Business which is a convenient cloud based storage system for your work related files. Although OneDrive for Business is an endorsed cloud file sharing solution for the campus, there are security practices that still must be followed to ensure the service is being used properly. OneDrive offers the following capabilities:

Store and share files

- Store up to 1 TB of data in the cloud
- 2 GB maximum file size
- Share files with other Mercy College Office 365 users
- Create and edit Microsoft Office files in the cloud with Office Web Apps (Word, Excel, PowerPoint, OneNote)

Access and synchronize files easily

- Access files using web browsers or mobile devices
- Access files directly from Microsoft Office desktop applications
- Synchronize your local files with files in OneDrive document libraries (with appropriate client software installed)

Please see guidelines for acceptable use below:

How to Use OneDrive Securely

Secure all computers or devices you are using to access OneDrive.

- Ensure virus/malware detection software is installed with the latest definitions.
- Do not log into your workstation or device as an administrator (unless absolutely necessary).
- Keep your operating system and software up-to-date.
- Password-protect your workstation or device and use idle-time screen saver passwords where possible.
- Don't sync files to a machine or device that is not issued and secured by the college.
- Don't store personal files in OneDrive.

Best Practices for sharing files

- Use folders to share groups of files with others online.
- Share files with specific individuals, never with “everyone” or the “public”.
- Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.
- Remember that once a file is shared with someone and they download it to their device, they can share it with others.
- Remove individuals when they no longer require access to files or folders.

Confidential Data

It is up to you to ensure you are abiding by FERPA standards when using the service. When in question check policy guidelines before moving confidential data to OneDrive for Business.

Confidential data if accessed by unauthorized entities could cause personal or institutional financial loss or constitute a violation of statute, act or law. Examples of confidential data include but are not limited to:

- Social Security Numbers
- Bank account or credit card numbers
- Data covered by the Family Educational Rights and Privacy Act (FERPA)
- Data covered by the Health Insurance Portability and Accountability ACT (HIPAA)
- Trade secrets or information that may be purchased for the creation of a patent
- Login/password credentials

Sensitive Data

Sensitive data may be stored and shared in OneDrive, but must be stored and shared in a secure manner.

Sensitive data is information generally used internally at the college or with its authorized partners. If released to unauthorized individuals would not result in any financial loss or legal compliance issues but would negatively impact the privacy of the individuals named or the integrity or reputation of the college. This includes but is not limited to the following:

- Employees who have chosen to suppress their directory information.
- Identities of donors or other third party partner information maintained by the college not specifically designated for public release.
- Proprietary financial, budgetary or personnel information not explicitly approved by authorized parties for public release.
- Emails and other communications regarding internal matters which have not been specifically approved for public release.

Unclassified Data

Unclassified data may be stored and shared in OneDrive, but must be stored and shared in a secure manner.

Data that does not meet the criteria as confidential, sensitive or private as defined above shall be considered non-classified data. Please note that this classification does not imply that the data does not need to be properly managed. Such data may be subject to open records requests.

Below are a few laws that govern the use and protection of data:

- **Sensitive data** is any data that is regulated by law or limited by contractual agreements between the college and other business partners.
- The **Family Educational Rights and Privacy Act** (FERPA) covers all student data. The college can disclose without consent directory information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance, as long as the student's disclosure preferences are honored. If any data is present that has been flagged for nondisclosure, or if the disclosure option is not checked and enforced, the data (along with all other student data that is not considered directory information) is considered sensitive.
- The **Gramm-Leach-Bliley Act** (GLB Act), officially known as the Financial Modernization Act of 1999, includes privacy provisions to protect consumer information held by financial institutions. Because of student loan activity, a college is considered a financial institution under the GLB Act. FERPA compliance places the college in compliance with FTC privacy rules under the GLB Act.
- The **Health Insurance Portability and Accountability Act of 1996** (HIPAA) is a federal law establishing national standards for the privacy and security of an individual's health information. This is information created or received by a health care provider or health plan, including health information or health care payment information plus information that personally identifies the individual patient or plan member, including:
    - A patient's name and e-mail, Web site and home addresses
    - Identifying numbers, including Social Security numbers, medical records, insurance numbers, biomedical devices, vehicle identifiers, and license numbers
    - Full facial photos and other biometric identifiers
    - Dates, such as birth date, dates of admission and discharge, or date of death
- **Payment Card Industry (PCI) Standard** is a contractual agreement between a college and its merchant bank. The agreement covers handling of credit card numbers, magnetic stripe contents, card verification code numbers, and expiration dates. In addition to the standards outlined above for sensitive systems, PCI requires extra security and has its own set of standards.