Guidelines for Data Storage and Collaboration

Introduction:

Faculty, staff and students have a number of options available for collaboration and file storage. The best choice among these options comes from carefully considering the purpose—particularly the type of data being handled/stored, the kind of collaboration/sharing activity to be undertaken and who will be participating. To help guide selection, the chart below outlines the options JMU provides and the types of data storage and collaboration activities for which they are best suited. This guidance supports university policy regarding data stewardship (see JMU Policy 1205) and incorporates several basic principles:

Highly Confidential Data *is not to be collected or stored outside the JMU central systems without specific approval of the university data managers and Information Technology*. This means that highly confidential data is not to be stored or shared using many of the options outlined below.
Protected Data *that includes Personally Identifiable Information (PII) may not be shared with individuals outside the university without specific approval of the university data managers, appropriate data custodians, and Information Technology.*
This means that when using one of these options, PII is to be shared/made available ONLY to persons who have a JMU eID and password.
University Data *should be stored using university-managed/contracted services*. This means that (other than for instructional purposes), JMU data storage and collaboration activities are to be performed using JMU-provided services such as those outlined below.

Overview of Services:

Office 365 is JMU's Microsoft cloud offering and includes a number of capabilities. The primary storage options included in Office 365 are SharePoint Online, OneDrive for Business, and Teams:

> **SharePoint Online** is specifically designed for document storage and collaboration. Backups are for service recovery purposes only, and one should not expect to have individual files restored. Deleted files are recoverable from the recycle area for up to 93 days. In certain cases, Personally Identifiable Information (PII) may be stored in SharePoint Online. However, the person doing the sharing must receive prior approval from the appropriate JMU Data Manager, appropriate Data Custodians, and Information Technology to access and share the data to be included in the site. JMU eIDs will be required for access to the data and to the SharePoint Online site. JMU IT will configure the site to prevent sharing with those who do not have a JMU eID.
> **OneDrive for Business** is an individual file storage and synchronization service available to faculty, staff and students hosted by Microsoft but managed by the university. Users may store, access, synchronize and share their files without assistance from IT. Backups are for service recovery purposes only, and one should not expect to have individual files restored. Deleted files are recoverable from the recycle area for up to 93 days.
> **Teams** is a collaboration and productivity tool that is included with Office 365. With Teams, you can chat with individuals or groups, hold video meetings, make audio/video calls, store and share files, and integrate with other applications. The file space also creates a SharePoint site so the files can be accessed with either Teams or SharePoint. Deleted files are recoverable from the recycle area for up to 93 days. In certain cases, Personally Identifiable Information (PII) may be stored in SharePoint Online. However, the person doing the sharing must receive prior approval of the appropriate JMU Data Manager, appropriate Data Custodians and Information Technology to access and share the data to be included in the site. JMU eIDs will be required for access to the data and to the SharePoint Online/Teams site.

JMU File Shares (N: and other lettered drives other than OneDrive) provide on-premises file storage for individuals and departmental groups. The JMU file shares are directly managed by JMU and provide basic document sharing and full backup/recovery capabilities.

Canvas is the university's learning management system and is the preferred option for collaboration in support of instruction.

Faculty, staff and certain registered affiliates automatically receive access to their individual/departmental file shares as their eIDs are established. Access to other groups/department shares can be made available upon request. Students also automatically have access to Office365 (SharePoint Online, OneDrive for Business, Teams) through their Dukes account, and access to Canvas through their eID (based on course enrollment.) Other options may be available to students as necessary upon request. For additional information on using these services, see Frequently Asked Questions

Type of Data and Collaboration Activity		UNIVERSITY-MANAGED SERVICES					Comments
		JMU File Shares	Office 365			Canvas	
			SharePoint Online	OneDrive for Business	Teams		
		available to JMU employees and certain registered affiliates	available to JMU employees and certain registered affiliates	available to JMU employees, students and registered affiliates	available to JMU employees, students and registered affiliates	available to JMU instructors and students in relation to their courses	
Type of Data Being Stored or Used	**Highly Confidential Data**	✓	✓		✓		Access to Highly Confidential data is restricted to those persons with specific approval of the university data managers. Such data may be stored temporarily on JMU File Shares, in SharePoint and Teams with special permission but may not be stored on individual hard drives, personally owned devices.
	Protected Data	✓	✓		✓		Protected data is generally available to those employees and registered affiliates with a well-defined "need to know" and as authorized by university data managers. Protected data that incorporates Personally Identifiable Information (PII) may be shared ONLY with those with a JMU eID and password
	Public Data	✓	✓	✓	✓		Public data is that portion of university data that is available in and outside the university community without restriction

Type of Collaboration Activity							
	Individual file store and backup	✓					Individuals approved to use Highly confidential data may store it temporarily in individual JMU File Shares. IT recommends that faculty and staff documents be stored in JMU File Shares rather than your local hard drive
	Collaborate on documents with other faculty and staff		✓	✓	✓		While basic document sharing can be accomplished using JMU Files Shares, collaboration is better accomplished using SharePoint. OneDrive for Business allows individuals to share data with others without requesting a separate collaboration space
	Collaborate with colleagues outside of the University			✓			OneDrive for Business allows for Sharing without IT assistance.
	Collaborate on documents with students in your course					✓	Canvas is the university's learning management system and is the preferred option for collaboration in support of instruction.
	Collaborate with a working group or committee		✓	✓	✓		On-going committees benefit from the collaboration tools that SharePoint provides.
	Collaborate with students not in your course		✓	✓	✓		OneDrive for Business allows for sharing without IT assistance.
	Share a OneNote Notebook with others at JMU			✓	✓		

References:

Data Stewardship Policy (JMU Policy 1205) establishes general methods and responsibilities for control and appropriate stewardship of university data.

Data Stewardship Standard defines procedural requirements developed in cooperation with the university's data managers to provide consistent control and security relative to a particular data item. These standards apply across all information systems and uses of university data.

Highly Confidential Data is restricted university data that, due to legal restrictions or potential risk, is available only on a very limited basis. University data managers have access to this data, and only with special security precautions.

Personally Identifiable Information (PII) is data that, on its own or with other information, may be used to identify, contact, or locate a single person, or to identify an individual in context.

Protected Data: Personally identifiable information or other university data worthy of protection and discretion in its distribution and use. University data managers generally approve individual access to protected data by employees for a specific business use. Data in this category is subject to the general security provisions associated with university data.

Public Data is university data openly available to anyone without university credentials or restrictions (e.g. list of university course offerings, publicity and news articles, published directory information, etc.)