

STORAGE	DATA AT REST ALLOWED?	DATA IN TRANSIT REQUIREMENTS	RETENTION REQUIREMENTS	DISPOSAL REQUIREMENTS
Filing Cabinets, Desk, Notebooks, Paper	YES, with limitations. Review business process to determine if PII is necessary to be collected. Use an alternate identifier. Keep confidential files and papers covered/closed when in public areas. Must be stored in a secure area.	Do not leave unattended if in an unsecured area. Review		Paper containing confidential data should be shredded or deposited in designated confidential paper repository. Follow applicable disposal guidelines found at: www.fortlewis.edu/recordsmgmt
FLC IT Department Managed Database	YES, with limitations. Collect the least amount of data necessary. Data should be accessed via individual user accounts. Protect your account credentials, use a strong password or two factor authentication.	Must be via an encrypted connection, such as https.	Collect and store the least amount of data necessary, for the least amount of time necessary. Follow applicable retention guidelines found at: www.fortlewis.edu/recordsmgmt	Follow applicable disposal guidelines found at: www.fortlewis.edu/recordsmgmt Delete data when it is no longer required to be retained.
Unencrypted database, documents, spreadsheets or files stored on FLC IT Department managed laptop, workstations, mobile devices or tablets	NO. Never store PII here.	NO. Never upload, transfer or post PII here.	CAUTION: If PII is found here, immediately contact the IT department.	CAUTION: If PII is found here, immediately contact the IT department.
ENCRYPTED Database, documents, spreadsheets or files stored on FLC IT Department managed workstation	YES. Contact the IT department to verify that your system is encrypted. Idle screen saver enabled and password protected. Protect devices from theft or loss.	CAUTION: Do not upload, transfer or post educational records on unsecured Wi-Fi networks. Do not leave device unattended in unsecure areas.	Collect and store the least amount of data necessary, for the least amount of time necessary. Follow applicable retention guidelines found at: www.fortlewis.edu/recordsmgmt	Return unused, damaged or end of life devices to Help Desk. Follow applicable disposal guidelines found at: www.fortlewis.edu/recordsmgmt

Databases, documents, spreadsheets or files on NON-FLC provided workstations, laptops, mobile devices, or tablets.	NO. Never store PII here.	NO. Never upload, transfer or post PII here.	CAUTION: If PII is found here, immediately contact the IT department.	CAUTION: If PII is found here, immediately contact the IT department.
Data stored on removable media: CD's, DVD's, Flash Drives	NO. Never store PII here.	NO. Never upload, transfer or post PII here.	CAUTION: If PII is found here, immediately contact the IT department.	CAUTION: If PII is found here, immediately contact the IT department.
FLC IT Department managed email account	NO. Never store PII here.	NO. Never upload, transfer or post PII here.	CAUTION: If PII is found here, immediately contact the IT department.	CAUTION: If PII is found here, immediately contact the IT department.
NON-FLC managed email account (i.e. Gmail, yahoo, etc.)	NO. Never store PII here.	NO. Never upload, transfer or post PII here.	CAUTION: If PII is found here, immediately contact the IT department.	CAUTION: If PII is found here, immediately contact the IT department.
Social Media Accounts	NO. Never store PII here.	NO. Never upload, transfer or post PII here.	CAUTION: If PII is found here, immediately contact the IT department.	CAUTION: If PII is found here, immediately contact the IT department.
FLC IT Department managed network shares: Department Share	YES, with limitations. Store here only if permissions to the file share or folder are restricted to only those authorized to view the information. Collect and store the least amount of data necessary, for the least amount of time necessary.	Any systems attached to network shares must have idle screen saver enabled and password protected. Protect device from theft or loss. Lock workstation screen i		

**FLC IT Department provided Office 365
OneDrive**

YES, with limitations.
Permissions to the file share or folder must be restricted to only those authorized to view the information. Collect and store the least amount of data necessary, for the least amount of time necessary.

Must use FLC supported web browser.
Remove site permissions from individuals when they no longer need access to the data.

When possible do not store reports or spreadsheets of data that can be easily pulled from the data store on demand. Follow applicable retention guidelines found at:
www.fortlewis.edu/recordsmgmt

Delete files when they are no longer needed. Follow applicable disposal guidelines found at:
www.fortlewis.edu/recordsmgmt

Dropbox, Google Docs or other NON-FLC