THE OHIO STATE UNIVERSITY

Institutional Data
Permitted Data Usage By Activity
Office of the Chief Information Officer

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

The table below shows which classifications of institutional data are permitted for specific data user activities.

Activity		Data Classification								
					Restricted (S4)					
		Public (S1)	Internal (S2)	Private (S3)	ORC SSN #, driver's license	HIPAA health information	GLBA financial data	Export Control	PCI credit card #	Other IDs Med Center ID
SHARE EXTERNALLY[1]	Fax	✓	✓	✓	⚠	⚠	⚠	✗	✗[2]	⚠
	OSU Website[3]	✓	✓	✗	✗	✗	✗	✗	✗	✗
	Cloud Storage, OneDrive	✓	✓	✓	⚠[4]	✗	⚠[4]	✗	✗	✗
	Microsoft Teams	✓	✓	✓	⚠[4]	✗	⚠[4]	✗	✗	✗
STORE[5]	Portable Storage Media, OSU Managed	✓	✓	⚠	⚠	⚠	⚠	⚠	⚠	⚠
	Portable Storage Media, Not OSU Managed	✓	✓	✗	✗	✗	✗	✗	✗	✗
	Portable Device, OSU Managed	✓	✓	⚠	⚠	⚠	⚠	⚠	⚠	⚠
	Portable Device, Not OSU Managed	✓	✓	⚠[6]	✗	✗	✗	✗	✗	✗
	Network Storage, OSU Managed	✓	✓	✓	⚠	⚠	⚠	⚠	⚠	⚠
	Cloud Storage, OSU Approved	*Requires contract through OSU Purchasing and approval of the Security Advisory Board. Then refer to terms of the specific service.* ***For list of OSU approved cloud services, click here.***								
	Cloud Storage, Buckeye Box	✓	✓	✓	✓	✗	✓	✗	✗	✓
	Cloud Storage, OneDrive	✓	✓	✓	⚠[4]	✗	⚠[4]	✗	✗	✗
	Microsoft Teams	✓	✓	✓	⚠[4]	✗	⚠[4]	✗	✗	✗
	Cloud Storage, Others	✓	✗	✗	✗	✗	✗	⚠[7]	✗	✗
	Paper	✓	✓	✓	⚠	⚠	⚠	⚠	⚠	⚠

[1] Data must only be shared with explicitly defined collaborators who have a business requirement to access the data.
[2] Exceptions can be approved by Office of Treasurer.
[3] Websites require access control such that only those persons authorized to access data are capable of doing so.
[4] The data of this type that is shared externally must be encrypted at the file level.
[5] All storage devices are subject to the OSU Information Security Standard.
[6] Consult local IT support for protection guidance before storing Private data on portable devices.
[7] Permitted as specified contractually or in the Technology Control Plan.

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

Legend

✔	*Permitted if security controls for data classification are followed*
⚠	*Permitted **only** if encrypted (electronic) and/or regulatory compliant (paper, fax, etcetera)*
✖	*Not permitted*

Examples (May include but are not limited to…)

Portable Storage Media	Portable storage media includes optical media (e.g., CDs or DVDs), magnetic media (e.g., backup tapes or diskettes), disk drives (e.g., external, portable, or disk drives removed from information systems), and flash memory storage devices (e.g., SSDs or USB flash drives).
Portable Device	Portable devices include portable client systems (e.g., laptop computers) and mobile devices (e.g., mobile phones, personal digital assistants (PDAs), and tablet computers).
Network Storage	NAS (Network Attached Storage), Remote Disk Drives (peer-to-peer), “Departmental Servers”