Platform	LEVEL 1 PHI/HIPAA-regulated	LEVEL 1 PCI/Credit Card	LEVEL 1 SSNs	LEVEL 1 FERPA-regulated	LEVEL 1 all other sensitive data	LEVEL 2 Internal data
BIONIC	NO	Consult with LITS*	Yes	Yes	Yes	Yes
OnBase	NO	Consult with LITS*	Yes	Yes	Yes	Yes
Workday	NO	Consult with LITS*	Yes	Yes	Yes	Yes
OnBoard	NO	NO	NO	Yes	Yes	Yes
Moodle	NO	NO	NO	Yes	Yes	Yes
Bryn Mawr websites/blogs	NO	NO	NO	NO	NO	Consult with LITS*
Bryn Mawr email/ calendar	Only if email is encrypted.	Only if email is encrypted.	Only if email is encrypted.	Yes	Yes	Yes
Non-BMC email services	NO	NO	NO	NO	NO	NO
Computer hard drive (and Crashplan backups)	NO	NO	NO	Yes	Yes	Yes
External storage device (USB drives, etc.)	Only if drive is encrypted.	Only if drive is encrypted.	Only if drive is encrypted.	Only if drive is encrypted.	Only if drive is encrypted.	Yes
Mobile device file storage	NO	NO	NO	NO	Only if device is kept up to date, encrypted, and password-protected.	Only if device is kept up to date encrypted, and password-protected.
Shared Network File Storage (S:, etc.)	NO	NO	Consult with LITS*	Yes	Yes	Yes
Microsoft 365 Apps (OneDrive, Forms, Teams, etc.)	NO	NO	NO	Yes	Yes	Yes
Non-BMC cloud storage (DropBox, Google Drive)	NO	NO	NO	NO	NO	NO
BMC-licensed generative AI tools	NO	NO	NO	Yes	Yes	Yes
Non-BMC licensed generative AI tools	NO	NO	NO	NO	NO	NO
Wufoo	NO	NO	NO	NO	NO	Consult with LITS*
Formsite	NO	Consult with LITS*	NO	Consult with LITS*	Consult with LITS*	Consult with LITS*
Qualtrics	NO	NO	NO	Consult with LITS*	Consult with LITS*	Yes

Notes:

See Bryn Mawr's Data Handling Policy for definitions and example of each data classification level.

Level 3 Public Data can be stored in any of the platforms listed.

Identifiable human subject research data must be stored in compliance with approved IRB protocol.

See Ask Athena for guides to encrypting external devices and email.

*Email help@brynmawr.edu or call the LITS Help Desk at 610-526-7440 to set up a consultation.