DATA HANDLING POLICY

BRYN MAWR COLLEGE

POLICY STATEMENT

This policy states the guiding principles for information stewardship and a framework for classifying and handling confidential information and applies to all members of the Bryn Mawr College community.

The College and its individual community members are expected to responsibly manage, handle, and use institutional information or data for instruction, research, service, and administration. While such information or data may be accessed from, or stored on, a College-owned, personally-owned, or third-party computer or device, this expectation of responsibility remains in force.

- **Institutional data** consists of all information that is created, collected, licensed, maintained, recorded, used, or managed by the College, its employees, or any person or agent working on behalf of the College, regardless of the ownership or origin of the information.
- An **institutional (or College-owned) system** is any server, computer, mobile device, network, or storage media owned, rented, or licensed by the College to store and access institutional data.

This College policy is intended to ensure the integrity, availability, and protection of institutional data without impeding legitimate, authorized access to, and use of, institutional data and systems.

Members of the Bryn Mawr community working with or using institutional data or systems in any manner must comply with the Bryn Mawr College Acceptable Use Policy.

DATA CLASSIFICATION

Because of the nature of the College's mission and activities, every department and faculty member has some degree of access to confidential information during the normal course of work. Each person and office is expected to:

- Understand the nature of confidential information in their care
- Manage that data with safeguards proportional to the degree of confidentiality
- Understand the consequences that might result from improper handling or unauthorized access

Data Classification	Description	Examples (each community member or department will have its own data list)	Consequences of Improper Handling or Unauthorized Access
Level 1: Regulated and Other Sensitive Data	Personally Identifiable Information (PII) and information protected by law, regulation, contract, binding agreement, or industry requirements. Information intended for very limited distribution on a need-to-know basis within the Bryn Mawr community.	• Social security numbers, birth dates, bank information or any personal, financial or specific information that could be used to steal identity or financial resources • Student records governed by FERPA • Healthcare information governed by HIPAA • Credit card information governed by PCI standards • Research data covered by formal agreements or contracts with the College • Tenure and promotion files • Personnel files • Accounts payable records • Compensation data • Special review and audit reports • Contracted research • Library patron and circulation records	May include legal sanctions, fines, and penalties for the College; violations of personal privacy; financial and/or reputational loss; potential lawsuits; for research data, loss of access to critical data sources or funding; violation of personal privacy
Level 2: Internal Data (Administrative and Community Data)	Information limited to distribution to members of the Bryn Mawr community who need the data to support their work. Information intended for the Bryn Mawr community. Information at this level will not contain regulated information, but may be restricted to some or all members of the Bryn Mawr community.	For documents which contain no level 1 data • Internal memos and emails • Planning documents • Meeting minutes • Licensed library resources	May include financial and reputational loss; loss of productivity; loss of access to resources; violation of agreements
Level 3: Public Data	Information intended for the public. Information at this level will not contain regulated or confidential information.	• Press releases and publications • Information posted on open websites and social media	Publicly posted information must not pose any significant harm to the College, checking materials for accuracy and civil discourse is important to avoid reputational loss

BEST PRACTICES

EMPLOYEE TRAINING

College employees, particularly those who use or access confidential information (Level 1) must have training which includes an overview of applicable laws; recommendations on how to avoid or address known risks, password security and encryption; appropriate methods of record storage and backup; proper methods of record disposal; and College policies and guidelines related to data security and stewardship.

Supervisors should direct employees to appropriate training resources, and LITS is available to consult.

DATA PROTECTION

Confidential College information must be maintained in the safest environment consistent with educational, research, service, or operational needs. Store confidential data in properly secured locations—see the Data Handling Storage Guidelines [on last page of PDF following policy]. If you use a mobile device to access College data, the device must be properly secured with a passcode and encryption. Use print-release functionality when printing confidential documents to shared printers/copiers. Departments and individuals are responsible for ensuring data is backed up to protect against loss due to equipment or technical failures. Consult with LITS if you have questions about how to back up data. Access to the information and/or the information storage equipment or areas must be limited to those with an appropriate business reason for such access. Supervisors will ensure that authorizations for access to confidential information are up to date for their departments as employees are hired, change roles, or depart.

While this policy focuses mainly on handling of data in electronic formats, handling of data in print formats is equally important.

- Staff must ensure the confidentiality and security of files, reports, and any other printed documents. Such documents must not be left unattended in public places or common areas.
- Storage areas, file rooms, and file cabinets with confidential information must be locked at the end of the day or whenever the area will be unattended.
- When printing confidential documents on shared printed, use secure print release.
- All printed documentation containing confidential information must be shredded when discarded or no longer needed.

PASSWORDS

Access to electronic information must be protected by strong passwords. Passwords must never be shared with anyone. Refer to the College's Acceptable Use Policy.

SECURITY UPDATES AND PATCHES

The College is responsible for updating core systems, servers, and network infrastructure and will do so as per the schedule posted at http://www.brynmawr.edu/computing/documents/SystemMaintenancePolicy.pdf

Updates and patches must be applied on a timely basis on both College-owned and personal computers and devices. Updates and patches designated as critical by the software vendor must be applied as soon as reasonably possible.

ANTIVIRUS PROTECTION

The College supports and maintains antivirus software for all College desktop devices. Employees must ensure they are using current antivirus protection software on any device they use for College business; contact LITS for College recommended options.

PERSONALLY OWNED DEVICES

Use a properly secured device to gain remote access to confidential College data. Do not use devices shared with others for accessing confidential College information. Avoid downloading confidential information to personal devices and avoid transmitting such data over the internet (e.g., forwarding via email).

SECURE DATA DELETION

Information no longer necessary for educational, research, service, or operational needs and not necessary to retain by law or College policy must be securely deleted as a regular business process or once discovered.

EMAIL FORWARDING

For community members with email accounts, all official College electronic correspondence will come to you via your Bryn Mawr email address. Each individual is responsible for promptly receiving official correspondence by accessing their Bryn Mawr email.

Faculty and Staff: Faculty and staff may not systematically forward email to external accounts. Any faculty or staff member who is also an alumna/us or who holds other status must remove any forwarding in the email system and any alumnae/i forwarding in Bionic for the time that they are employed. Forwarding email increases the risk of exposing sensitive data.

Shared (or departmental) email addresses being used for official College purposes may not be forwarded outside brynmawr.edu.

Students: Students who prefer to use another account are responsible for forwarding email and configuring outside accounts to accommodate Bryn Mawr College email. Bryn Mawr cannot guarantee delivery or recovery of emails forwarded to outside accounts (see http://techdocs.blogs.brynmawr.edu/1800). Students who forward their Bryn Mawr email to an external account are responsible for regularly checking their Bryn Mawr email via that personal account. Graduate and undergraduate students holding campus positions that involve access to privileged information may be required to remove email forwards.

Please note that popular personal email accounts such as Gmail, Outlook.com, etc. are not offered under the same terms of service as your institutional email account and do not promise confidentiality or compliance with any standard; use caution and read terms of service carefully.

STORAGE

See Data Handling Storage Guidelines [on last page of PDF following policy].

POLICY VIOLATION

Members of the Bryn Mawr community who either intentionally or unintentionally violate this policy and/or the Acceptable Use Policy risk loss of access to some or all College information resources and may be subject to other penalties and

disciplinary action, both within and outside of the College. The College may refer suspected violations of applicable law to appropriate law enforcement agencies.

RELATED POLICIES

- Acceptable Use Policy – Library & Information Technology Services Resources
- Digital Millennium Copyright Act (DMCA) Policy
- Webpage Policy
- Web Privacy Policy
- InCommon Federation Participant Operational Practices

DATA HANDLING STORAGE GUIDELINES

	Level 1						Level 2	Level 3
Storage	***HIPAA/PHI***	***PCI/Credit Card***	***SSN***	***Identifiable human subject research data***	***FERPA***	***Other Confidential Data (personnel files, ID numbers, compensation data, etc.)***	***Internal Data (Internal memos and emails, planning documents, licensed library resources, course data, etc.)***	***Public Information (Information posted on open websites, etc)***
H: Drive	NO	NO	NO	Comply with approved IRB protocol	Yes	Yes	Yes	Yes
Shared Network File Storage (S:, etc.)	NO	NO	Consult with LITS*	Comply with approved IRB protocol	Yes	Consult with LITS*	Yes	Yes
Microsoft 365 OneDrive	NO	NO	NO	Comply with approved IRB protocol	Yes	NO	Yes	Yes
Bryn Mawr College email/calendar	NO	NO	NO	Comply with approved IRB protocol	Yes	Consult with LITS*	Consult with LITS*	Yes
Moodle	NO	NO	NO	Comply with approved IRB protocol	Yes	Consult with LITS*	Consult with LITS*	Yes
Local computer hard drive / desktop	NO	NO	NO	Comply with approved IRB protocol	Yes	Yes	Consult with LITS*	Yes
Mobile device	NO	NO	NO	Comply with approved IRB protocol	NO	NO	Consult with LITS*	Yes
DropBox / Google Drive / non-BMC cloud services	NO	NO	NO	Comply with approved IRB protocol	NO	NO	Consult with LITS*	Yes
Bryn Mawr Web Servers and blogs	NO	NO	NO	Comply with approved IRB protocol	NO	NO	Consult with LITS*	Yes
Social Media	NO	NO	NO	Comply with approved IRB protocol	NO	NO	NO	Use discretion.
Peripheral storage devices (USB drives, etc)	NO	NO	NO	Comply with approved IRB protocol	NO	Consult with LITS*	Consult with LITS*	Yes
Non-BMC email services	NO	NO	NO	Comply with approved IRB protocol	NO	NO	NO	Yes
BIONIC	NO	Consult with LITS*	Yes	Comply with approved IRB protocol	Yes	Yes	Yes	Yes
OnBase	NO	Consult with LITS*	Yes	Comply with approved IRB protocol	Yes	Yes	Yes	Yes
Director's Desk	NO	NO	NO	Comply with approved IRB protocol	Yes	Yes	Yes	Yes

* Contact the LITS Help Desk to arrange a consultation: help@brynmawr.edu or x7440.

NOTE: Educational resources including Securing the Human are available via LITS as orientation to data handling topics, such as working with regulated data.