Library Services Privacy Policy

I. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. Within Maxwell Library the right to privacy is the right to open inquiry without having the subject of one’s interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. This library's privacy and confidentiality policy is in compliance with applicable federal, state, and local laws including Code of Massachusetts Regulations under 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth.

The library’s commitment to privacy and confidentiality has deep roots not only in law but also in the ethics and practices of librarianship. In accordance with the American Library Association’s Code of Ethics: “We protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted.”

The library user rights outlined below are based on what are known as the five “Fair Information Practice Principles.” These principles outline the rights of Notice, Choice, Access, Security and Enforcement.

II. Library Services’ Commitment to Users

Library Services is committed to protecting user privacy and confidentiality rights when library resources are used, personally identifiable information (PII) is collected, or PII is provided by users or by parties associated with Bridgewater State University (e.g. the Registrar’s Office or Human Resources). PII is defined by Section 17.02 of 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth:

- first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number.
number, or credit or debit card number, with or without any required security code, access code, personal identification number or password ….

A. Notice & Openness

Library users have the right of notice about the policies governing the amount and retention of personally identifiable information, and about why that information is necessary for the provision of library services.

Library Services publicly posts and openly acknowledges the privacy and information-gathering policies of this organization. Whenever policies change, notice of the changes will be disseminated to users.

Library Services will not create unnecessary records, will not retain records not needed for the fulfillment of its mission, and does not utilize practices that might place personally identifiable information on public view.

Library Services may collect usage data in order to improve services and to better participate in (or contribute to) university initiatives regarding teaching, learning, and research.

Information that may be gathered and retained about library usage include the following:

- Circulation information
- Interlibrary loan and document delivery contact information
- Electronic access information
- Bibliographic Instruction session information
- Library web forms, chat sessions, email messages

B. Choice & Consent

Library Services keeps all personally identifiable information confidential and will not share, sell, license, or disclose personal information to any third party without user consent unless compelled to do so under penalty of law or to comply with a court order.

If a user is affiliated with Bridgewater State University, then Library Services receives personally identifiable information from the Office of the Registrar (student information) and the Office of Human Resources (employee information) for operational use only. Library Services may also receive information directly from a user in order to create and update library user records.

To activate library borrowing privileges, Library Services creates a link between a user’s personally identifiable information and the items borrowed by scanning the user’s
Bridgewater State University identification card or similar valid identification card with photograph such as a driver’s license.

When using the library’s website and licensed subscription electronic resources, a user may be prompted or required to provide a Bridgewater State University username, email address, library barcode number, pin, and/or password to be authenticated as a currently affiliated user or as a guest user.

When using certain library services, resources, or collections, a user may be asked to show identification or provide personally identifiable information on forms or logs that are retained as needed.

C. Access by Users

Library users must update their personally identifiable information to ensure that library operations function properly. Such functions may include notification of overdue items, holds, etc. Bridgewater State University students can view and update their personally identifiable information through the student management system. Faculty and staff can view their personally identifiable information through the employee management system. All other users not currently affiliated with Bridgewater State University may contact Maxwell Library directly to update their information.

For services that require the use of personally identifiable information, users are entitled to view and update their information. A user may view personal information online or in person and request that it be updated if it is not correct. In both instances, a user may be asked to provide some sort of verification of identity.

D. Data Integrity & Security

Data Integrity: The data Library Services collects and maintains must be accurate and secure. Library Services’ staff take reasonable steps to assure data integrity, including: using only reputable sources of data; providing users access to their own personally identifiable data; updating data whenever possible to ensure its currency and accuracy; utilizing middleware authentication systems that authorize use without requiring personally identifiable information; destroying untimely data or converting them to anonymous forms.

Data Retention: Library Services protects personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services. Information that should be regularly purged, shredded, or anonymized includes personally identifiable information on library resource and services use, circulation history, forms, and security/surveillance tapes and logs.
**Tracking Users:** Library Services ensures aggregate summary data is stripped of personally identifiable information and/or deleted when it is no longer needed. Library Services staff do not ask visitors to the library or website to identify themselves or reveal any personal information unless they are borrowing materials, requesting services, registering for programs or events, or using portions of the library’s website restricted to registered borrowers such as licensed content. Library Services uses Google Analytics, a web tracking and analytics service, to better understand website usage, to improve the user experience and access to services. Google Analytics operates through the use of cookies, a text file placed on one’s computer that contains information about one’s use of library websites. The information stored in the cookie is transmitted to and stored by Google. This information is for analytical and improvement use only. Library Services does not provide any of this information to third parties. To opt-out of Google Analytics on your personal computer, install a browser add-on created by Google: [https://tools.google.com/dlpage/gaoptout](https://tools.google.com/dlpage/gaoptout).

**University Information Technology Systems and Services:** Use of institutional wireless (Wi-Fi) and wired connections as well as use of computers within the library is managed by the Information Technology Division of Bridgewater State University. Library Services does not have access to any information stored and collected through these services and systems.

**Third Party Security:** Library Services does license products, tools, resources, and specialized services for operational use from third-party vendors that have individual privacy policies and license agreements. Library Services reviews all such policies and agreements to ensure user privacy protections are in place and adhered to. However, interactions with these systems are governed by the third-party vendors’ individual privacy policies. Check the privacy statements of specific vendors to learn how data is stored and used, or contact Library Services to request a license agreement for any specific vendor. Library Services does not use cookies to collect information about users and library website use. However, Google Analytics and many vendors of licensed resources may require a user accept cookie files. Refusing to accept cookies may degrade or impede the full functionality of certain services or resources.

**Security Measures:** Library Services uses technical and managerial methods to protect against unauthorized access, loss, use, or disclosure of collected data. Library Services encrypts and encourages its third-party vendors to encrypt internet traffic via the use of SSL certificates and emerging options or through the use of passwords and auditing tools for proper access to data stored on computers and/or servers. The managerial measures used by Library Services include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes.

**Staff Access to Personal Data:** Only authorized staff with assigned confidential passwords have access to personal data stored in the computer systems for performing
their essential duties and fulfilling their responsibilities. Library Services employees will not share any personal data collected from users with any other party except where required by law enforcement agencies or by court order. Library Services does not sell, lease, distribute or in any way release free of charge personal information to individuals, companies, or other higher education institutions.

E. Enforcement & Redress

Library Services will not share data on individuals with third parties unless required by law or court order. Library Services conducts regular privacy audits in order to ensure that all library programs and services are enforcing its privacy policy. Users who have questions, concerns, or complaints about how Library Services manages privacy and confidentiality rights should file written comments with the Director of Library Services. The Director will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures before responding in writing.

Only the Director and/or the Director’s designee can receive or comply with requests from law enforcement officers or with court orders. The Director will confer with University legal counsel before determining the proper response to any law enforcement requests or served court orders. The Director will not make library records available to any individual, local, state or federal agency unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction that shows good cause and is in proper form. All library staff and volunteers will refer any law enforcement inquiries to the Director of Library Services.