# Bridgewater State University Student Handbook 2024-2025

Home / Policies and Procedures / Responsible Use of Information Technology

## *Purpose*

The purpose of this policy is to delineate the responsible use of information technology at Bridgewater State University (BSU). Information technology includes but is not limited to computer networks, network servers, personal computers, workstations, voice and video networks, cloud (internet-based) services, transmission systems, software, and digital information provided by Bridgewater State University.

## *Scope*

This policy applies to all students, employees, contractors, and third parties who access BSU systems.

## *Policy*

BSU provides information technology resources to students, employees, contractors, and third parties in support of the University's mission of teaching and learning and to conduct official University business. The University, however, may limit, restrict, or extend computing/information network privileges and access to its resources as it may determine appropriate. As with all University assets, information technology is to be used in ways consistent with state law and overall University policy.

Responsible use of information technology requires that you:

1. Respect the rights of others by complying with all University policies regarding sexual, racial, and other forms of harassment, and by preserving the privacy of personal data to which you have access. University resources, from any location, may not be used to transmit content that is discriminatory, defamatory, fraudulent, or obscene; or which violates any federal or state law.

2. Use only accounts and communication facilities which you are duly authorized to use and for the purposes for which they were intended; for example, you should not use University information technology to run a private business for financial gain or to solicit others for commercial ventures, religious or political causes or outside organizations.

3. Acknowledge that personal use of the University's technology resources is not prohibited, provided the personal activity does not violate federal, state, or University policies or regulations, and does not disrupt, distract from, or interfere with the conduct of University business; or impose a burden on the University.

4. Respect all pertinent licenses (including software licenses), copyrights, contracts, and other restricted or proprietary information. Use only legal versions of copyrighted software in compliance with vendor license requirements.

5. Respect the integrity of computing systems and data; for example, by not intentionally developing programs or making use of already existing programs that harass other users, or infiltrate a network or computing system, and/or damage or alter the components of a network or computing system, or gain unauthorized access to other facilities accessible via the network.

6. Respect and adhere to any state or federal law which may govern the use of information technology or communication networks.

7. Acknowledge that the privacy and confidentiality of electronic information transmissions cannot be guaranteed; for example, electronic mail is generally not secured and is vulnerable to unauthorized access and modification.

8. Acknowledge that authorized University personnel may examine computing resources and data. Examples include but are not limited to communication systems, files, email, learning management systems, cloud services, database, and other software applications or services for reasons including but not limited to troubleshooting hardware and software problems, preventing or investigating unauthorized access and system misuse, response to cybersecurity threats, assuring compliance with software copyright and distribution policies, campus safety, cyberbullying, academic continuity, and complying with legal and regulatory requests for information.

## Enforcement

Information technology users who violate this policy will be subject to University disciplinary processes and procedures. Privileges to use information technology may be revoked. Illegal acts may also subject users to prosecution by law enforcement authorities.

Questions and comments regarding this policy should be directed to:

Division of Information Technology Boyden Hall Room 209 Bridgewater State University Bridgewater, MA 02325 508-531-2555
itsupport@bridgew.edu

## Roles and Responsibilities

| Role | Responsibility |
|---|---|
| Management Team | Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented. Review this policy periodically and update as needed in response to environmental and/or operational changes. |
| All Users | Understand and adhere to this policy. Use Bridgewater State University resources in only those methods, which have been identified as acceptable by this policy. Immediately report suspicious activities or violations of this policy to their manager or the IT Manager. |
| Responsible Department | Information Security Office |
| Policy Owner | Vice President of Information Technology & Chief Information Officer |

## Revision History

This section contains comments on any revisions that were made to this document and the date they were made.

| Version Number | Issued Date | Approval | Description of Changes |
|---|---|---|---|
| 1.0 | 04/1/2016 | Vice President of Information Technology & CIO | Initial Policy |
| 1.1 | 06/02/2020 | Vice President of Information Technology & CIO | Policy review with minor language revisions. |
| 1.2 | 07/01/2022 | Vice President of Information Technology & CIO | Policy review with language clarifications. |

Reviewed 8/2024 by Steve Zuromski, Vice President of Information Technology & CIO