



Internet Safety Policy

Computers will be available to students at Bridgewater Academy. Along with computer use also includes access to the internet. Our goal is to provide these services to students in order to promote resource sharing, innovation and communication.

This internet safety policy provides for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

Technology Protection Measures

Student use of computers must be in support of education and research and must be consistent with educational objectives of Bridgewater Academy. Accordingly, internet access at Bridgewater is filtered and monitored on an ongoing basis to protect against access by adults and minors to visual depictions that are obscene, child pornography, or harmful to minors. Filtering may be disabled for adults who are engaged in bona fide research or other lawful purposes upon receiving special permission from the Director and/or the School Board.

Documentation of technology protection measures will be retained for at least five years after the latest date of service.

Students will be educated in appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response. The safety and security of students when using electronic mail, chat rooms, and other forms of direct electronic communications is a priority at Bridgewater Academy; As such:

- 1) Students will sign computer use and safety agreements annually.
- 2) Students are strictly prohibited to:
 - Access or create files or materials without authorization.
 - Attempt to hack into any school systems.
 - Access or create offensive, profane, or pornographic files.
 - Plagiarize works or violate copyrights or trademarks.
 - Attempt to bypass computer security.
 - Have food or drinks near computers.
- 3) There will not be an expectation of privacy in files, disks, documents, internet history, etc., which have been used or created with Bridgewater equipment.



BRIDGEWATER ACADEMY

- 4) All documents, files, folders created with school hardware/software remain the intellectual property of Bridgewater Academy.
- 5) Vandalism will result in appropriate disciplinary action. Vandalism includes, but is not limited to: abusive overloading of data on the server, uploading or downloading or creation of computer viruses, any malicious attempt to harm or destroy the property.
- 6) Security is a high priority because of multiple users. Students are prohibited to use another individual's account or login information other than his/her own at any time. Any security concerns must be reported to the director, teacher/supervisor or system administrator.
- 7) Personal information is restricted, password protected, and stored only on the school servers, teachers will sign disclosures regarding the use, and dissemination of personal information regarding students. Only authorized personnel have access to student information. No personally identifiable information about students will be shared without written consent of a parent.
- 8) The use of the computers and internet is a privilege, not a right. Inappropriate use of these resources may result in disciplinary action (including the possibility of suspension or expulsion), and/or referral to legal authorities. The director, teacher/supervisor or systems administrator may limit, suspend or revoke access to electronic resources at any time.
- 9) Users are liable for any misuse of the systems.
- 10) Parental permission is obtained for the publication of student work, and photos.

Documentation of the Internet safety policy will be retained for at least 5 years after the last day of the funding year in which the policy was relied upon to obtain E-Rate funding.