ACCEPTABLE USE POLICY

The Board of Education provides a wide range of technology resources to advance the educational mission of the Bethlehem Central School District (the District) and manage District operations. Pursuant to District Policy #8630 concerning District Technology Resources and Data Management, the Board has established this Acceptable Use Policy (AUP).

Capitalized terms in this Policy have the same meaning as the same terms set forth in Policy #8630.

This AUP is applicable to all Users of District Technology and Data, including all students, staff, Board members, volunteers, vendors, and visitors who are authorized to access District Technology and Data. All use of District Technology and Data is subject to this AUP and the District Code of Conduct, regardless of whether such use occurs at school or outside of school. Pursuant to the Code of Conduct and this AUP, all Users of District Technology are required to conduct themselves in a responsible, decent, ethical, and polite manner.

The superintendent, working in conjunction with the District's director of Technology (DOT) shall prepare an appropriate Regulation to define the specific acceptable uses of District Technology and Data (the AUP Regulation). The AUP Regulation shall be made available to all Users, who shall be required to acknowledge receipt of, and agree to comply with, the AUP Regulation before being provided access to District Technology and Data.

Any violation of the AUP Regulation may be grounds for discipline, which may include termination of access to District Technology and Data or other appropriate sanctions under the circumstances.

Cross-Reference:	1130.1 Social Media Guidelines 4526.1 Internet Safety 8630 Technology Resources and Data Management 8635 Information Security Breach & Notification
Rescinds:	4526 Computer Use in Instruction 4526.2 Acceptable Use
Adoption Date:	August 9, 2017

ACCEPTABLE USE REGULATION

This Acceptable Use Regulation (AUP Regulation) establishes the general rules for use of District Technology pursuant to the Acceptable Use Policy No. 4526 (AUP or Policy No. 4526) of the Bethlehem Central School District (the District).

Capitalized terms in this Regulation have the same meaning as the same terms set forth in Policy No. 4526.

I. Notice of User Rights and Limitation of District Obligations

A. *No Expectation of Privacy*. Users have no expectation of privacy regarding use of District Technology or storage of Data on District Technology, including, but not limited to, Data contained in any User account, on the District's computer network or authorized cloud computing solution, or on any device issued by the District to any student.

B. *Access Is a Privilege*. Access to District Technology and Data is a privilege, not a right. The District reserves the right to prohibit or limit any use that is not for educational purposes; interferes with the normal operation of the District; or violates any law, policy, or regulation.

C. *No Warranties*. The District makes no warranties of any kind, express or implied, relating to access to, or use of, District Technology or Data. Further, the District assumes no responsibility for the quality, availability, accuracy, nature, or reliability of the service and/or information provided. Users of District Technology use such technology at their own risk. Each User is responsible for verifying the integrity and authenticity of all information obtained through use of District Technology, including any information obtained from the Internet. The District is not liable for any claims, losses, damages, suits, expenses, or costs of any kind incurred, directly or indirectly, by any user or his/her parents and/or guardians arising out of the use of District Technology.

D. *Limits on Filtering Technology*. No Internet filtering/blocking software is 100 percent effective. The District is not responsible for failure of such software to block or prevent access to all potentially objectionable content.

E. *Limits on Security Controls*. No security controls are 100 percent effective to eliminate all threats. The District is not responsible for failure of any reasonable security controls to preserve the confidentiality, integrity, and availability of District Technology or Data.

II. Use of District Technology

A. *Educational and District Uses*. District Technology is provided to support student learning and manage the District's operations. All Users are expected to use District Technology for educational and other District purposes. Educational purposes include academic or classroom instruction, research, and other learning opportunities consistent with the District's educational mission.

B. *Prohibited Uses*. The following uses are specifically prohibited.
   1. Any use that violates this Regulation or any other District Regulation or Policy, including but not limited to the Code of Conduct [see Policy # 5300];
   2. Any use that violates applicable law;
   3. Posting any material or information that may result in disruption of normal school operations;
   4. Cyberbullying and/or harassing other Users [See Policy # 5810 (Cyberbullying) and Policy # 5300 (Code of Conduct)];
   5. Accessing, uploading, downloading, creating, or distributing pornographic, obscene, or sexually explicit material;
   6. Copyright infringement;
   7. Gambling;
   8. Vandalizing the account or Data of another User;
   9. Accessing another User's account or confidential records without permission;
   10. Attempting to read, delete, copy, or modify the electronic mail of other system Users and deliberately interfering with the ability of other system Users to send and/or receive email;
   11. Using another person's account name, with or without permission;
   12. Revealing the personal address, telephone number, or other personally identifying information of a student unless written permission has been given by a parent or guardian;
   13. Sharing your personal ID or password with another User;
   14. Using any methods or means to bypass the District's Internet filtering system, including, but not limited to, use of a Virtual Private Network (VPN);
   15. Intentionally or knowingly disrupting or damaging District Technology or Data, including creating, installing, sharing, or distributing a computer virus or similar damaging code, application, or program;
   16. Using District Technology for personal financial gain;
   17. Downloading, installing, or using software without permission;
   18. Email broadcasting or spamming;
   19. Using District Technology to send anonymous messages or files;
   20. Using a false/fictitious identity in any electronic communication; or
   21. Forging or attempting to forge email messages.

C. *Personal Devices*. Personal Devices owned by Users may be used to connect to the District's computer network, including wireless Internet access points maintained by the District. Personal Devices that may be used include, but are not limited to, laptop computers, smartphones, and tablets. All activities conducted while connected to the District computer network are subject to monitoring, copying, review, access, and storage by the District. The District is not liable for any damages, expenses, or costs associated with the use of a Personal Device to access District Technology, or in the event such a Personal Device is lost, damaged, or stolen.

D. *District-Issued Devices*. The District may issue devices to Students or Staff for use in school and outside of school. Parents and/or guardians, students, and Staff will receive (and must acknowledge receipt of and agree to follow) the specific guidelines regarding rights and responsibilities relating to use of these District-owned, leased, or controlled

devices. The District reserves the right to inspect or examine all District-issued devices to ensure compliance with this Regulation and other applicable policies and regulations.

E. *Internet Safety*. In accordance with the Children's Internet Protection Act of 2001 and the Protecting Children in the 21st Century Act of 2008, the District has adopted an Internet Safety Policy and a Regulation that specifically govern use of District Technology to access the Internet (4526.1/4526.1-R). All Users are required to abide by the requirements of the District's Internet Safety Policy and Regulation.

F. *Social Media*. The District has adopted Social Media Guidelines that specifically govern use of Social Media relating to the District and District activities (1130.1). All Users are required to abide by the requirements of the District's Social Media Guidelines.

G. *Data Storage*. The District uses a variety of approved solutions for storing Data. Some Data may be stored on servers located in the District, while other Data may be stored by third party vendors (for example, remote cloud storage). The District's director of Technology (DOT) is responsible for communicating to Users how and where Data should be stored.

H. *Security Incidents*. If a User identifies a security problem involving District Technology or Data, the User must notify the District's Information Technology (IT) staff or other responsible school official immediately. Under no circumstances should the User demonstrate the security issue to another User or encourage any other User to exploit or replicate the security problem.

III. **Violations**

A. Violations of the Acceptable Use Policy and this Regulation shall be reported to the building principal, who shall take appropriate action in accordance with authorized disciplinary procedures set forth in the District's Acceptable Use Policy or other applicable policies.

B. Penalties for students may include, but are not limited to, the restriction or revocation of computer access privileges, suspension, and other discipline consistent with the Code of Conduct.

C. Penalties for staff and other authorized Users may include, but are not limited to, revocation of computer access privileges and other discipline allowed pursuant to contract and/or law up to and including termination.

D. In addition, the District may pursue legal options for damage to District Technology or Data, or for other damages suffered by the District.

E. Violations that appear to be criminal in nature will be reported to the appropriate law enforcement authorities