TECHNOLOGY RESOURCES AND DATA MANAGEMENT REGULATION

This Technology Resources and Data Management Regulation (Regulation) establishes the general rules for procurement, management, and disposal of Bethlehem Central School District (the District) Technology Resources and Data pursuant to the District’s Technology Resources and Data Management Policy #8630.

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

Administration

1. The District’s Director of Technology (DOT) is responsible for overseeing the installation, management, use, and disposal of District Technology and Data.

2. Responsibilities delegated to the DOT include:

   A. Deploying, maintaining, and retiring of District Technology pursuant to the District’s multi-year technology plan and consistent with Policy # 6900 relating to disposal of District property;
   
   B. Identifying technology vendors to supply technology solutions that meet the requirements of the District’s multiyear technology plan and working to procure such technology solutions consistent with Policy # 6700 regarding purchasing;
   
   C. Developing guidelines for issuance and use of District-owned, leased, or controlled devices to students and staff, including use of such devices in school and outside the school setting;
   
   D. Monitoring, examining, and auditing use of District Technology, including the District’s computer network, to confirm compliance with all applicable District policies and regulations;
   
   E. Conducting due diligence on third-party suppliers, including cloud service providers, to confirm compliance with all applicable District policies and regulations;
   
   F. Developing and implementing procedures for backup and storage of Data, including facilitation of the District’s disaster recovery plan, compliance with Policy # 1120 (School District Records), and use of third-party cloud storage providers;
   
   G. Developing, acquiring, and implementing reasonable technical, administrative, and physical safeguards to protect the confidentiality, integrity, and availability of District Technology and Data;
   
   H. Maintaining all consents and/or acknowledgments signed by Users relating to Acceptable Use, Internet Safety, and Technology Resources and Data Management and documenting receipt of such consents in a database or other convenient format;
   
   I. Working with the superintendent and other appropriate school officials to ensure appropriate staffing for District Technology management functions;
   
   J. Disseminating and interpreting District policy and regulations governing District Technology and Data;
K. Providing notices, training, and educational materials relating to the appropriate use of District Technology and management of Data to Users;
L. Providing technical support to Users, including support for devices issued by the District to students for use both in school and outside the school setting;
M. Restricting and/or terminating access of any person to District Technology or Data for failure to comply with applicable policies and regulations; and
N. All other tasks necessary to implement and comply with policies and regulations relating to District Technology and Data

User Account Management

Student internet access is addressed in policy # 4526 and regulation # 4526-R, Computer Use for Instruction. District employees and third-party users are governed by the following regulations:

1. Staff, students, and Board members will be issued user accounts or otherwise be granted access to use District Technology appropriate to their needs in connection with instruction and operation of the District, which may include access to the District’s computer network, email, and cloud computing services.
2. From time to time, other Users with a legitimate need, including vendors or volunteers, may be issued accounts or otherwise granted access to use District Technology for a limited period of time and strictly limited to that User’s specific needs.
3. Prior to granting access to District Technology or Data, all Users shall be notified of their obligations, the limitations of their rights, and limitations of the District’s obligations with respect to District Technology and Data.
4. The DOT and/or his/her designee may retain master administrative passwords or use other means to access, inspect, monitor, suspend, or terminate any administrative or User account at any time and for any reason consistent with law and/or any District policy or regulation.

Adoption date: August 9, 2017
Revised date: September 23, 2019
Re-Adopted: October 16, 2019