

The Board of Education recognizes that computers are a powerful and valuable education and research tool and as such are an important part of the instructional program. In addition, the District depends upon computers as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the Board's expectations in regard to these different aspects of the District's computer resources.

### *General Provisions*

The Superintendent shall be responsible for designating a Director of Technology or his/her designee who will oversee the use of District computer resources. The Director of Technology will prepare in-service programs for the training and development of District staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

The designated purchasing agent for the District and the Director of Technology will be responsible for the purchase and distribution of computer software and hardware throughout the schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or District needs.

The Superintendent, working with the Director of Technology shall establish regulations governing the use and security of the District's computer resources. The security and integrity of the District computer network and data is a serious concern to the Board and the District will make every reasonable effort to maintain the security of the system. All users of the District's computer resources shall comply with this policy and regulation, as well as the District's Acceptable Use and Conduct (4526). Failure to comply may result in disciplinary action, as well as suspension and/or revocation of computer access privileges.

All users of the District's computer resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the District's computer network must not expect, nor does the District guarantee, privacy for electronic mail (e-mail) or any use of the District's computer network. The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's computer network.

### *Management of Computer Records*

The Board recognizes that since District data is managed by computer, it is critical to exercise appropriate control over computer records, including financial, personnel and student information. The Superintendent, working with the Director of Technology and the District's business official, shall establish procedures governing management of computer records. The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- encryption,
- user access and permissions appropriate to job titles and duties,
- disposal of computer equipment and resources (including deleting District data or destroying the equipment),
- inventory of computer resources (including hardware and software),
- data back-up,
- archiving of email effective January 31, 2012,
- record retention, and

- disaster recovery plans.

If the District contracts with a third-party vendor for computing services, the Superintendent, in consultation with the Director of Technology and/or Business Official and/or School Attorney, will ensure that all agreements address the procedures listed above, as applicable, and that all agreements are in compliance with Education Law §2-d.

#### *Review and Dissemination*

Since computer technology is a rapidly changing area, it is important that this policy be reviewed periodically by the Board and the District's external auditor. The agreement governing appropriate computer use (4526 E.1 and 4526 E.2) will be made available to staff and students.

*Cross-ref:* 1120, School District Records  
4526, Computer Use for Instruction  
4526.1, Internet Safety  
6600, Fiscal Accounting and Reporting  
6700, Purchasing  
8635, Information Security Breach and Notification

Adoption date: August 18, 2008  
Revised: December 12, 2011  
Revised: November 10, 2014  
Revised: March 28, 2016  
Reviewed: August 28, 2017