ICHABOD CRANE **8630**

TECHNOLOGY RESOURCES AND DATA MANAGEMENT

The Board of Education recognizes that computers, computer networks and other technological resources are needed for instruction, as well as management of District business. The Board also recognizes that District Technology is used to create, store and transfer data created by students, staff and other authorized Users. This Technology Resources and Data Management Policy sets forth the Board's expectations regarding management of District Technology and Data.

I. Definitions

A."District Technology" includes:

1. All District owned, leased or controlled computer equipment, software, applications and other electronic devices (including but not limited to laptops, smartphones, databases, webpages, and email accounts, social media accounts, etc.);
2. The District's computer network, including network components located on school premises and remote components, such as District authorized cloud storage solutions (e.g., Google Classroom); and
3. District owned, leased or controlled wired and wireless connections used to access the District's computer network or the Internet.

B."Data" includes:

1. Data accessed, created, compiled, stored or maintained on District Technology, regardless of whether such Data was created for District purposes and regardless of who owns the legal rights to such Data; and
2. Data accessed, created, compiled, stored or maintained on any District-authorized cloud storage solution, regardless of whether such Data was created for District purposes and regardless of who owns the legal rights to such Data.

C."Personal Device" includes any computing device not owned, leased or controlled by the District.

D."User" includes any person who is authorized to access District Technology or Data, including students, staff, board members, contractors and visitors.

II. Management Responsibilities

A. The Superintendent is responsible for designating a Director of Technology ("DOT") to oversee the installation, use, management, and disposal of District Technology and Data.
B. The Superintendent, working in conjunction with the designated purchasing agent for the District and the DOT, is responsible for:

1. Preparing a comprehensive multi-year technology plan for Board approval, which may be revised from time-to-time (subject to Board approval) to reflect changing technology and/or District needs;
2. Purchasing, distributing, and/or installing District Technology pursuant to the Board-approved technology plan, including devices that may be issued directly to students for their use both in school and outside of school;

3. Adopting reasonable and appropriate procedures relating to the access, use, storage and disposal of District Technology and Data;
4. Adopting reasonable and appropriate procedures relating to damage caused by any person using District Technology or to whom a District owned, leased or controlled device is issued;
5. Adopting reasonable and appropriate Internet filtering technologies required to comply with the District's Internet Safety Policy and Regulation (4526.1/4526.1-R);
6. Adopting reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of District Technology and Data;
7. Preparing reasonable and appropriate notices and training programs for Users relating to appropriate use of District Technology, Data, and Internet Safety;
8. Adopting reasonable procedures to create and manage administrative and individual User accounts, including maintaining District access rights to all such accounts;
9. Adopting reasonable procedures to ensure that third party vendors comply with all District technology-related policies, procedures and guidelines;
10. Implementation of all other District policies and regulations relating to District Technology and Data, including but not necessarily limited to:

- Policy 4526 and Regulation 4526-R Acceptable Use of District Technology;
- Policy 4526.1 and Regulation 4526.1-R Internet Safety; and
- Policy 8635 and Regulation 8635-R Security Incident Notification.

Cross-Reference:

4526 Acceptable Use
4526.1 Internet Safety
8635 Security Incident Notification

Effective Date: June 2, 2020

TECHNOLOGY RESOURCES AND DATA MANAGEMENT REGULATION

This Technology Resources and Data Management Regulation establishes the general rules for procurement, management and disposal of 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.

I. **Administration**

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

B. Responsibilities delegated to the DOT include:

1. Deploying, maintaining and retiring of District Technology pursuant to the District's multi-year technology plan and consistent with Policy No. 6900 relating to disposal of District property;

2. Identifying technology vendors to supply technology solutions that meet the requirements of the District's multi-year technology plan and working to procure such technology solutions consistent with Policy No. 6700 regarding purchasing;

3. Developing guidelines and procedures relating to damage caused by any person using District Technology or to whom a District owned, leased or controlled device is issued;

4. Developing guidelines for issuance and use of District owned, leased or controlled devices to students and staff, including use of such devices outside the school setting.

5. Monitoring, examining and auditing use of District Technology, including the District's computer network to confirm compliance with all applicable District policies and regulations;

6. Conducting due diligence on third party suppliers, including cloud service providers, to confirm compliance with all applicable District policies and regulations;

7. 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;

8. Developing, acquiring and implementing reasonable technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of District Technology and Data;

9. Maintaining all consents and/or acknowledgements 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;

10. Working with the Superintendent and other appropriate school officials to ensure appropriate staffing for District Technology management functions;

11. Disseminating and interpreting District policy and regulations governing District Technology and Data;

12. Providing notices, training and educational materials relating to the appropriate use of District Technology and management of Data to Users;

13. Providing training to Staff responsible for supervising students to ensure that students receive training on compliance with District Technology policies and regulations;

14. 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;

15. Restricting and/or terminating access of any person to District Technology or Data for failure to comply with applicable policies and regulations; and

16. All other tasks necessary to implement and comply with policies and regulations relating to District Technology and Data.

II. User Account Management

A. 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.

B. 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.

C. 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.

D. 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.

Effective Date: June 2, 2020