Responsible Office: Office of Information Technology

BOARD POLICY 7210

INFORMATION TECHNOLOGY SERVICES AND OPERATIONS

PURPOSE

The Board of Trustees ("Board") is committed to supporting teaching and learning, business operations, and administrative functions through information technology services and operations. Such services and operations shall be conducted in an equitable manner, comply with relevant laws, and be informed by industry best practices. This policy shall govern the Washoe County School District's ("District") protocols for information technology management.

POLICY

1. Guiding Principles

    a. The Board has established a commitment to 21st Century learning through Board Policy 7200. In doing so, the District acknowledges the need to establish and maintain protocols for information technology services and operations.

    b. The District shall promote equity of technology access and opportunities and support for students, faculty, and staff through technology practices and procedures that secure the District network while empowering schools with student-centered technologies.

    c. Information technology services and operations needs shall be clearly identified and budgeted to provide an appropriate level of service and support to District technology users.

2. Guiding Practices

    a. A District Technology Plan shall be established and maintained to guide the deployment of information technology services and operations to best meet the needs of students, schools, and District departments.

        i. The District Technology Plan shall be reviewed annually to ensure compliance with changes to state and federal laws and regulations, as well as applicable best practices as recognized nationally through such organizations as the National School Boards

Association (NASB) and their member school districts, the National Institute of Standards and Technology (NIST), the United States Department of Education's (USDoE) Privacy Technical Assistance Center (PTAC), the Consortium for School Networking (CoSN), and the International Society for Technology in Education (ISTE).

b. The Superintendent may create administrative regulations and procedures to establish appropriate practices and implementation for the District's information technology services and operations. These administrative regulations and procedures may include:

   i. data access and protection, including management of account access and passwords, Guest network access, account management, remote access, and access by third parties;

   ii. data retention, including backups and storage, data disposal, retention limits, and responsibilities, litigation hold, data classification, email retention, e-discovery and access to employee accounts, and data loss prevention;

   iii. information security, including information security monitoring, information security risk management, physical access, email encryption, student and staff data privacy, development of family data privacy educational resources, and computer evidence collection;

   iv. applications support, including department responsibilities for applications support,

   v. disaster recovery, business continuity, and incident response, including disaster recovery planning, business continuity planning, and breach identification and recovery;

   vi. District website management, including website content management, and website accessibility;

   vii. network protection, including network and infrastructure protection, server protection, and endpoint protection; and

   viii. Information technology systems acquisition and development, including acquisition, non-standard equipment, and excess equipment.

DEFINITIONS

1. Applications – refers to a computer software program hosted by an information system.

2. Business Continuity – refers to the approach used to identify, and ensure the continuity of, vital business functions, especially in the case of disaster events.

3. Cybersecurity – refers to the ability to protect or defend District information resources and services utilizing cyberspace—the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

4. Data Classification – refers to the process of organizing data by relevant categories so that it may be used and protected more efficiently and effectively.

5. Data Disposal and Destruction – refers to the process of destroying and/or removing data from District information services to ensure that sensitive data cannot reasonably be accessed or used for unauthorized purposes.

6. Data Governance – refers to a set of processes that ensures that data assets are formally managed throughout the enterprise.

7. Data Loss Prevention – refers to a system's ability to identify, monitor, and protect data from unauthorized use and transmission.

8. Data Retention – refers to the process used to manage and protect important data to remove outdated and duplicated information, and to avoid potential civil, criminal, and financial penalties.

9. Disaster Recovery – refers to the process for responding to and recovering from a major hardware or software failure, or destruction of facilities, to resume the processing of critical applications.

10. District Network – refers to all District technology devices as a whole, including but not limited to the District wide area network (WAN), local area networks (LANs), firewalls, routers, switches, hubs, cabling, computers and peripherals, and telecommunications devices.

11. E-discovery – refers to the process of seeking, locating, securing, and searching for data with the intent of identifying and using it as evidence in a civil, criminal, or administrative case or process.

12. Guest Wireless Network – refers to filtered and managed access to the Internet through the District's technology resources.

13. Information Security – refers to actions undertaken to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

14. Litigation Hold – refers to the process of preserving all forms of relevant information when litigation is reasonably anticipated.

15. Remote Access – refers to the ability to access the District network from a physical or virtual location outside of the District network.

DESIRED OUTCOMES

1. Through the implementation of this policy, the Board desires to establish a comprehensive framework for information technology services and operations that:

    a. empowers learning and teaching with technology in support of digital and 21st Century learning; and

    b. ensures the District can plan and provide important information technology services and operations, including information technology management, data access and protection, data retention, information security, applications support, disaster recovery, business continuity, incident response, District website management, network protection, and systems acquisition and deployment.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This policy reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:

    a. Board Policy 7200, 21st Century and Digital Learning

    b. Board Policy 7205, Information Technology – Data Access

2. This policy complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC), to include:

    a. Chapter 388, System of Public Instruction, and specifically:

        i. NRS 388.134, Policy by school districts for provision of safe and respectful learning environment and policy for ethical, safe and secure use of computers; provision of training to board of trustees and school personnel; posting of policies on Internet website; annual review and update of policies

3. This policy complies with federal laws and regulations, to include:

    a. Children's Internet Protection Act: 20 U.S.C. 6801 and 47 U.S.C. 254(h).

    b. Broadband Data Improvement Act, Title II, Protecting Children in the 21st Century Act

c. Children's Online Privacy Protection Act

REVIEW AND REPORTING

1. This document shall be reviewed as part of the bi-annual review and reporting process, following each regular session of the Nevada Legislature. The Board of Trustees shall receive notification of any required changes to the policy as well as an audit of the accompanying governing documents.

2. Administrative regulations, and/or other associated documents, will be developed as necessary for the consistent administration of this policy.

REVISION HISTORY

Date	Revision	Modification
12/11/2018	1.0	Adopted