Chuck Shaw Technical Center
Data Privacy, Safety and Security Plan
2023-2024

Purpose

The purpose of this plan is to outline the acceptable use of technology that is used in the District. These standards are in place to protect the District's information resources and technology and the Employees and Students that must use these resources. Inappropriate use, in violation of the provisions of the School Board's technology policies, exposes the resources and users to risks, including virus attacks, identity theft, denial of services, loss of data, and misuse of resources and information. School Board Policies 3.29 and 8.123 govern the use of District technology.

Privacy and Safety of Data

The computer systems network is managed at the district level, and appropriate staff is provided to maintain the equipment and provide emergency repairs. All staff are required to take mandatory IT Security Awareness training annually. The following District policies address privacy, safety, and security of data.

Policy 3.29 Acceptable Use of Technology - The purpose of this policy is to set forth terms and conditions as well as standards and guidelines for the acceptable uses by District employees and School Board members (hereinafter collectively referred to as employees) of Palm Beach County School District technology resources and other technology when conducting District business. The policy also provides for employee use of e-signatures and electronic notarizations when authorized. This policy does not prohibit or restrict public access to inspect data and information on publicly available District technology resources.

Policy 5.50 Student Education Records- The purpose of this policy is to provide uniform procedures to challenge the content of student education records to ensure that the records are not inaccurate, misleading, or otherwise a violation of privacy or other rights, pursuant to Fla. Stat. § 1002.22 (2)(c). Persons on behalf of the School District who handles student education records are responsible for being acquainted with this policy and -the federal and Florida student education records laws, regulations, and rules, which this policy implements and supplements.

Security of Data

Bulletin# PD22-141 CIO FY22 Annual IT Security Audit Review- The audit is a formal review of user access to Peoplesoft, TRIRIGA, and the Student Information System (SIS). Principals, directors or higher-level administrators must confirm the appropriateness of each employee's user access based on current job responsibilities and current job title. PeopleSoft permissions for staff with access above Basic Self-Service need to be reviewed. All TRIRIGA and Student Information System (SIS) permissions except for auto=provisioned teacher roles need to be reviewed.

Computer System and Network Reliability

The SDPBC Technical Plan addresses computer system and network reliability in Chapter 3. The District's network is currently a geographically dispersed redundant network of two (2) Data Centers: FHESC and SITV. This geographically redundant architecture is provided by the internet service providers used by SDPBC (AT&T and Florida LambdaRail (FLR). The infrastructure has two (2) points of presence; one located in Ft. Lauderdale/Miami and a single point of presence on Florida LambdaRail provided by Palm Beach County.

The CSTEC IT specialist ensures our campus technology devices, such as computers, iPads, and Chromebooks, are backed up regularly. The SDPBC backs up the school's network infrastructure, conducts regular updates, and ensures reliability.

Emergency Backups

The SDPBC Technical Plan addresses computer system and network reliability in Chapter 3. The District's System Response Center (SRC) is the main center for network monitoring, performance, and dashboards. This center is designed to monitor the network at each of the 180+ school locations and the many District offices. Its main goal is to respond to the business and educational needs of teachers, students, and employees while ensuring a safe and reliable network. The SDPBC maintains the CSTEC networks, backs up our system, and conducts timely updates. The SDPBC IT department is responsible for continuous uptime, acceptable performance, and overall improvement of the back-end infrastructure (servers, network equipment, phones, etc.) required to maintain the District's technology and mission-critical systems.

Evaluated Annually

The Technology Plan is evaluated annually by the District IT department and is revised if necessary.

Available to Administration, Faculty, Staff and Students

The SDPBC Technology Plan is available to faculty, staff, and students on the District website.