

Board of Education

Kate I. Noble, President
Sarah K. Boses, Vice President
Dr. Carmen L. Gonzales, Secretary
Roman "Tiger" Abeyta, Member
Juan Blea, Member

Superintendent of Schools

Dr. Christine E. Griffin



**Board of Education Meeting
Cover Sheet
August 27, 2026**

Item Title: Second Reading of New Policy 547 Cybersecurity

Summary: Policy 547 establishes a districtwide framework for cybersecurity and information security and sets expectations for protecting SFPS information systems and data. The policy addresses access management, data protection, network and device security, vendor oversight, cybersecurity awareness, business continuity, incident response, and compliance. It also establishes the Board's role in setting cybersecurity expectations and receiving regular reports and assigns implementation of the policy to the Superintendent through administrative regulations.

Recommendation: It is recommended that the Board of Education approve Policy 547, Cybersecurity, on second reading and adopt the policy as presented.

Funding Source: Existing district operating and technology budgets, as applicable. Any future funding needs will be addressed through the district's regular budget process.

Cost Implication(s): There is no direct cost associated with the first reading or adoption of the policy. Implementation and continued improvement of the district's cybersecurity program may result in future costs related to training, security systems and services, risk assessment, monitoring, backup and recovery, and other cybersecurity safeguards.

Staff Implication(s): District staff will be responsible for implementing the policy and related Administrative Regulation, including maintaining appropriate cybersecurity safeguards, providing cybersecurity awareness education, supporting incident response and recovery, managing vendor security requirements, and monitoring and improving the district's cybersecurity practices.

Submitted by: Juan Blea, Board Member
Roman "Tiger" Abeyta, Board Member
Jaime Holladay, Deputy Superintendent
Michael Hagele, Chief Information and Strategy Officer

Indicate if Signature is Required by: No signature is required as part of the Board action. Following adoption, the policy should be processed according to the district's standard policy approval procedures.

Additional Documentation Attached: Yes ☒ No ☐

1 Santa Fe Public Schools (SFPS) serves students across its campuses and relies on digital technology
2 for instruction, administration, communications, and student records. The Board of Education is
3 committed to protecting the confidentiality, integrity, and availability of district information systems
4 and data. The Superintendent shall implement this policy through administrative regulations
5 consistent with applicable law.

6
7 This policy applies to all individuals who access, manage, or interact with SFPS information systems
8 or data, including:

- 9 ● All district employees including full-time and part-time
- 10 ● Board members in their official capacity
- 11 ● Students using district-issued or district-accessed technology
- 12 ● Third-party vendors, contractors, and service providers with access to SFPS networks or data
- 13 ● Volunteers with authorized system access

14
15 This policy covers all SFPS-owned, leased, or managed technology assets, including networks,
16 servers, workstations, mobile devices, cloud services, and software applications, regardless of
17 physical location.

18
19 The Board shall establish cybersecurity expectations, provide appropriate resources, review this
20 policy periodically, and receive regular reports regarding the district's cybersecurity program. The
21 Superintendent is responsible for implementing this policy through administrative regulations.

22
23 The District shall maintain reasonable administrative, technical, and physical safeguards to protect
24 information systems and data. Safeguards shall include access management, data protection, network
25 and device security, secure use of technology, vendor oversight, user awareness, and business
26 continuity measures.

27 The District shall protect confidential information, including student and employee records, in
28 accordance with applicable federal and state law. Sensitive information shall be safeguarded from
29 unauthorized access, disclosure, alteration, or destruction.

30
31 The District shall maintain the capability to identify, respond to, recover from, and document
32 cybersecurity incidents. Significant incidents shall be reported to the Board as appropriate and in
33 accordance with applicable law.

34 District users shall receive cybersecurity awareness education appropriate to their role.

35 Violations of this policy may result in disciplinary action, loss of technology privileges, contract
36 remedies, and referral to law enforcement as appropriate and consistent with applicable law, district
37 policy, and collective bargaining agreements.

38 This policy shall be read with the Acceptable Use Policy, Student Code of Conduct, Employee Code
39 of Conduct, Records Management Policy, and other related Board policies.

40

41

42 **References:** Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; Children's
43 Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506; Children's Internet Protection Act,
44 Pub. L. No. 106-554 and 47 USC 254 *et seq.* (CIPA); New Mexico Inspection of Public Records Act
45 (NMSA 1978, §§ 14-2-1 through 14-2-12); Health Insurance Portability and Accountability Act, Pub.
46 L. No. 104-191 (HIPAA); National Institute of Standards and Technology (NIST) Cybersecurity
47 Framework.

48

49 Policies 321, 511 and 513.

50