HILLDALE PUBLIC SCHOOLS BOARD OF EDUCATION POLICY	*Technology I.6* Adopted: July 2020

CYBERSECURITY

The District takes seriously the safety and security of its students and staff, which includes electronic security. Therefore, it is the policy of the District to have in place measures to prevent unauthorized access to its computer networks and to prevent the online theft, disclosure, use, or dissemination of personally-identifiable information stored on its computer networks (a "security incident").

Cybersecurity Protection Measures Generally

The Superintendent or designee shall be responsible for the design and monitoring of measures to prevent and respond to unauthorized or unlawful access to or use of data on the District's computer networks ("preventative measures"). These measures shall include identifying network vulnerabilities, developing disaster recovery and business continuity plans, establishing clear procedures that comply with this policy, and educating all stakeholders and users on the importance of computer network security. Additionally, the storage of personally-identifiable information stored on District computer networks should be designed so that in the event of a data breach incident, the following data elements associated with the first name or first initial and last name of an individual are either encrypted or redacted: (a) social security number, (b) driver license number or state identification card issued in lieu of a driver license, or (c) financial account number, or credit card number, in combination with any required security code, access code, or password that would permit access to the financial account of the individual.

Security and Monitoring

The District will take reasonable efforts to maintain computer network security, whether threatened by security breach, human error, hardware malfunction, or otherwise. The Superintendent or designee shall be responsible for securing and actively monitoring the District's computer network ("network") to identify, contain, mitigate, and report any security incident, which may include contracting with a third party for such services. However, any staff member who suspects or becomes aware of a security incident shall immediately notify the Superintendent or designee.

The Superintendent or designee shall also be responsible for designing, or having in place, adequate preventative measures, including perimeter and access controls, to regulate digital traffic between the District's computers and external entities. To the extent practicable, the electronic transmission of personally-identifiable information should be encrypted or redacted. Additionally, the Superintendent or designee shall ensure the District's network and all District computer equipment are protected from malicious software attacks such as viruses,

ransomware, spyware, and malware by commercial grade cybersecurity software and appropriate and regularly-updated software, including timely installation of necessary software patches.

The Superintendent or designee shall annually report to the board of education regarding the adequacy of the District's preventative measures, including any security incidents that have occurred, the District's responses to those incidents, and subsequent improvements to network security. The Superintendent or designee shall also conduct vulnerability assessments to monitor the efficacy of the District's preventative measures and make ongoing improvements or updates to security protocols, systems, hardware, and software as necessary.

The Superintendent or designee shall also develop a disaster recovery or business continuity plan to be implemented in the case of a disaster or serious security incident which compromises the District's network and/or the data stored thereon. This plan shall include procedures for routinely backing-up District data to a secured, off-site location or onto appropriate backup media at a secure, off-site location. The District may contract with a third party for such services. At least [frequency, i.e., annually, semi-annually], the Superintendent or designee shall conduct contingency testing to ensure the speedy restoration of District systems and information in the event of a security incident or a disaster.

Response and Reporting

In the event of a security incident, Superintendent or designee shall immediately notify the Superintendent of Schools, and they, in consultation with the District's legal counsel, shall take such reasonable and appropriate steps as may be required, which may include notification to law enforcement and affected parties.. The Superintendent shall also notify the Board of Education of any security incidents as soon as practicable.

Education

The Superintendent or designee is responsible for providing annual information technology training to District personnel who have access to sensitive and personally-identifiable information. This training will emphasize such employees' personal responsibility for protecting the District's network and personally-identifiable information. Additionally and on an ongoing basis, the Superintendent or designee will provide guidance to all District employees on best practices to mitigate against the threats of a cyber-attack.

Reference: OKLA. STAT. tit. 74, § 3113.1; OKLA. STAT. tit. 24, §§ 161–166 ("Security Breach Notification Act"); 20 U.S.C. § 1232g, 34 C.F.R. Part 99 ("FERPA"); 47 U.S.C. § 254; 47 C.F.R. § 54.520 ("Children's Internet Protection Act"); 20 U.S.C. § 7131 ("Elementary and Secondary Education Act"); 15 U.S.C. § 7001