CYBER SECURITY POLICY

I. PURPOSE

The Lincoln School Committee seeks to always prepare for a wide variety of cyber threats and hazards in school settings and create a safe, secure, resilient, and accessible education digital infrastructure as provided by state and federal law. Lincoln strives to promote cybersecurity and make adherence to cybersecurity safeguards part of the school community culture. Lincoln seeks to protect all student information in adherence with all state and federal laws, including the Family Education Rights and Privacy Act (FERPA).

II. ENABLING AUTHORITY

The Lincoln School Committee hereby adopts this policy on cyber security to comply and be consistent with any applicable state and federal law or regulation regarding cyber security, as well as any federal and state guidance issued for schools, including the Children's Internet Protection Act (CIPA), FERPA, Protection of Pupil Rights Amendment (PPRA), and Children's Online Privacy Protection Act (COPPA).

III. POLICY

A. Definitions. For the purposes of this policy the following terms take on these meanings:

1. "Multi-Factor Authentication (MFA)" is a multi-layered security access management process that grants users access to a network, system, or application only after confirming their identity with more than one credential or authentication factor.

2. "Ransomware attacks" are a form of malware (malicious software designed to steal data and damage computer systems) frequently delivered through phishing scams to tempt users to click on a link that downloads malicious software that infects computers or systems.

3. "Data breaches" are leaks of sensitive, protected, or confidential data from a secure environment to an unsecure environment.

4. "Business Email Compromise (BEC) Scams" are a specific form of phishing when an email is sent that falsely claims to be a legitimate organization to deceive the recipient into visiting a fake Website and divulging sensitive information.

5. "Distributed Denial-of-Service (DDoS) Attacks" are cyberattacks in which a server is deliberately overloaded with requests until access is temporarily or permanently disrupted.
6. "Website and Social Media Defacement" are incidents in which unauthorized changes, such as the publication of inappropriate or offensive images or language, are published to a school or school district Website or social media account.
7. "Online Class and School Meeting Invasions" are situations in which a perpetrator accesses an online voice or video platform without authorization for the purpose of disruption.

B. Lincoln Public Schools will take a variety of actions to prevent, protect the school community from, mitigate the effects of, respond to, and recover from cyber threats that occur in the form of ransomware attacks, data breaches, DDoS attacks, website and social media defacement, online class and school meeting invasions, and any other cyber threat directed at the education system digital infrastructure.

IV. DEVELOPMENT OF PROTOCOL

The Superintendent of Schools shall develop a protocol to facilitate this policy.

TOWN OF LINCOLN SCHOOL COMMITTEE, Lincoln, Rhode Island

First Reading Approved: March 10, 2025
Second Reading Approved: April 21, 2025
Approved: April 21, 2025