COLCHESTER SCHOOL DISTRICT

POLICY: CYBERSECURITY

DATE ADOPTED: March 7, 2023

I. PURPOSE

The Colchester School District ("District") supports secure network systems, including security for all personally identifiable information that is stored on paper or stored digitally on District maintained computers and networks. This policy supports efforts to mitigate and respond to potential cybersecurity incidents that may cause harm to the district, schools, students, or employees.

The primary objective of this policy is to ensure user awareness and training of cybersecurity and their role and responsibility in protecting district data.

A. Effective information security requires the awareness and proactive support of all users, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and frauds, for example, which directly target individuals rather than IT and network systems.

B. Lacking adequate information security awareness, users are less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information in danger through lack of education and carelessness.

II. DEFINTIONS

Cybersecurity: The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Personally Identifiable Information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another or to infer someone's individual identity.

Security Breach: The unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information.

Incident: Any event that threatens the confidentiality, integrity, or availability of District information assets (electronic or paper), information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices.

Date Warned: January 13, 2023
First Reading: January 17, 2023
Second Reading: March 7, 2023

Users: Includes anyone who accesses the District's IT resources, on-site and/or via a remote location, and anyone who uses the District's IT devices either on or off-site.

III. RISK MITIGATION STRATEGIES

The following security measures shall be taken to help mitigate cybersecurity risks.

A. All users will immediately notify the Technology Department of any cybersecurity incidents and possible security breaches.

B. Secure passwords are used on all district computers and changed periodically.

C. All district devices shall be locked with a password when unattended and will automatically lock when idle.

D. All employees shall undergo annual cybersecurity awareness training which emphasizes their personal responsibility for protecting student and employee information. Cybersecurity training shall include, but not be limited to:

1. Phishing and ransomware

2. Email and messaging security

3. Password complexity and two-factor authentication

4. Personal identifiable information

5. Malware and virus protection

6. Safely sharing files with other entities

E. All employees with access to sensitive information must ensure that access and transfer of the information is secure.

F. All employees shall enable two-factor authentication on their Google account.

IV. INCIDENT RESPONSE MANAGEMENT

The superintendent or their designee shall develop incident response procedures to be implemented should a cybersecurity incident occur.