Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity

This document defines the computer security policy for the District's computer systems. The District's computing environment is defined as all computer equipment and related software owned and used by the District. All data in the computer systems of the District shall be considered District assets. Data will be handled as confidential information. Any use of this information shall relate only to authorized District use. This policy applies to all District employees, students, District contractors, school Board members, organizations and individuals accessing the District's systems. Violation of this policy may be grounds for suspension and termination of employment or student disciplinary action.

The District's computer network environment is provided for students and staff to access, organize, create, and communicate information in accordance with the District's vision and mission statement. Individual users of the District computers and networks are responsible and accountable for abiding by this policy. This policy outlines user responsibilities when using the District's information resources and to provide guidelines that will ensure the appropriate safeguarding of the confidentiality, integrity, and availability of physical assets and information stored, processed, or transmitted electronically. It is recommended that this policy undergo annual review to ensure that it reflects applicable current laws and regulations.

Definitions

The most common types of online threats include the following;

*"**Spoofing or Phishing**"* is a form of cyberattack and is the practice of sending legitimate-seeming emails to entice users to reveal personal information or click on links that install malicious software. Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source. Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information (passwords, credit card numbers, bank account information).

- ***Deceptive phishing*** are emails from legitimate-seeming companies asking the individual to verify his/her account and to enter personal details.
- ***Spear phishing*** is a more targeted form of phishing and typically involves sending an email that appears to come from a colleague or acquaintance. It contains an individual's personal information, such as position, name etc. to make the email appear more legitimate.
- ***Superintendent Fraud*** uses an email similar to the Superintendent's to get the recipient to send proprietary information.

"***DDoS or Denial of Service"*** is a distributed denial-of-service attack that occurs when multiple systems flood the bandwidth or resources of district servers. It occurs when a server is deliberately overloaded with requests such that the Website shuts down preventing access to the Website by users.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity

Definitions (continued)

"Data Breach" is the release of secure confidential information from a secure to an insecure environment that are then copied, transmitted, viewed, stolen or used in an unauthorized manner. Data breaches often occur with confidential information such as student records that may be inappropriately viewed or used by an individual who should not have access to the information.

"*Malware/Scareware"* Malware is illicit software that damages or disables computers or computer systems. Scareware is similar to malware and uses social engineering to cause fear or anxiety so that a user buys unwanted or unneeded software such as antivirus software.

"Ransomware" is a type of malicious software that encrypts the District's data and requires a ransom to be paid, typically in virtual currency such as Bitcoin, in order to regain access to the data. The threat of releasing the data is also sometimes made unless a ransom is paid. This threat may escalate to threatening emails sent to parents and students with ransom being demanded from the schools.

"Unpatched or Outdated Software Vulnerabilities" is when unpatched or outdated software has not been updated to include the latest software updates which then allows unauthorized users to gain access to information networks and systems.

"*Removable Media"* are media devices that can be connected to computers, such as thumb drives, CDs, DVDs, and external hard drives. These can be easily stolen or corrupted devices can be intentionally or unwillingly connected to computers. Once opened, files from the device can then infect the computer with malware.

The District needs to take a variety of actions to prevent, protect from, mitigate the effects of, respond to, and recover from the cyber threats identified in this policy. Therefore, the Board believes the following are integral parts of a proactive cybersecurity plan:

1. Students, teachers and staff, prior to accessing District networks or systems need to be aware of the policies regarding their use, incorporated in applicable student and staff acceptable use policies.

2. Technology staff shall be aware of local, state, and federal statutes and regulations about information security, privacy and storage of personally identifiable information.

3. All data shall be stored securely to comply with the Family Educational Rights and Privacy Act (FERPA).

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity (continued)

4. The District shall regularly back up its data in case of accidental or deliberate corruption or destruction of data. Backups should be maintained in a different location. Also storage of backups off-site should be considered.

5. Firewalls shall be created and an approved list of individuals who have access to district networks and systems shall be maintained.

6. District networks shall be monitored continually to assess the risk from cyber threats.

7. Notification of law enforcement shall occur after any incident, in addition to any individuals whose personal information may have been compromised.

8. Training and awareness programs shall be provided to staff, including but not limited to, good password practices, role-based access to information, safe practices, identification of threats, proper response to threats.

9. District vendors shall be required to maintain adequate security measures to protect student data in compliance with state and federal statutes and district policy.

The Superintendent or his/her designee shall be responsible for ensuring the District has the necessary components in place to meet the District's needs for information technology security.

The District may consider retaining expert outside consultants, including legal counsel, to conduct annual/periodic evaluations of the District's security risk management program, with findings shared with the Board.

The District's computer security systems shall not be circumvented or subverted in any manner, and any unauthorized duplication of copyrighted or District computer software, hardware, procedure manuals or other materials is prohibited.

Violation of this policy shall be grounds for suspension and/or termination of employment or student disciplinary action in accordance with applicable policies.

(cf. 3520 – Data Processing Services)
(cf. 3520.1 – Information Security Breach and Notification)
(cf. 3520.11 – Electronic Information Security)
(cf. 3520.12 – Data-Based Information Management System Confidentiality Policy)

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity (continued)

(cf. 3520.13 – Student Data Protection and Privacy/Cloud-Based Issues)
(cf. 5125 – Student Records)
(cf. 5145.15 – Directory Information)
(cf. 6162.51 – Surveys of Students/Student Privacy)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.

7-109 Destruction of documents.

10-15b Access of parent or guardians to student's records.

10-209 Records not to be public.

10-234aa Definitions.

10-234bb Contracts between boards of education and contractors re student data. Requirements. (as amended by PA 18-125)

10-234cc Requirements for operators re student data.

10-234dd Duties re unauthorized release, disclosure or acquisition of student data. (as amended by PA 18-125)

11-8a Retention, destruction and transfer of documents.

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

36a-701b Breach of Security re computerized data containing personal information. Notice of breach. Provision of identity theft prevention services and identity theft mitigation services. Delay for criminal investigation. Means of notice. Unfair trade practice.

46b-56(e) Access to Records of Minors.

Connecticut Public Records Administration Schedule V - Disposition of Education Records. (Revised 1983).

P.A. 16-189 An Act Concerning Student Privacy.

PA 17-200 An Act Making Revisions to the Student Data Privacy Act of 2016.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity

Legal Reference: Connecticut General Statutes (continued)

PA 18-125 An Act Concerning Revisions to the Student Data Privacy Act.

Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at 20 U.S.C.

Dept. of Educ, 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Educ. Provisions Act (20 U.S.C. 1232g) parent and student privacy and other rights with respect to educational records, as amended 11/21/96.

Protection of Pupil Rights Amendment (PPRA) 20 U.S.C. § 1232g (2014)
Children's Online Privacy Protection Act (COPPA) 15 U.S.C. §§6501 *et seq.* (2014)

Policy adopted: February 25, 2020

MONTVILLE PUBLIC SCHOOLS
Montville, Connecticut

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity

General Guidelines

1. Systems access shall only be given to verified District employees, students, contractors, parents/guardians, business partners, and other District authorized users who have acknowledged the District's acceptable use policy.
2. The use of District owned Information Technology (IT) equipment and resources subjects the user to applicable District policies.
3. No student, staff member, or patron shall have access to the system or use of the system without having a signed "acceptable use" form on file with the district. (or who have been made aware of the "Acceptable Use" policy. Students under the age of 18 must have the approval of a parent/guardian. This provision applies to access or use by either a District or personally owned computer.
4. System users are required to change passwords the first time the account is accessed.
5. Directors, managers, and principals shall approve the appropriate level of system access for each employee for whom they have responsibility for.
6. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are responsible for all activity under their account. There is no reasonable expectation of personal privacy in the use of account files. Such files are district property and are subject to review and monitoring to ensure the responsible use of electronic files consistent with the terms of this policy.
7. Employee system access shall be electronically removed upon the employee's employment separation from the District.
8. All requests for system access will be made to the appropriate administrator or teacher.
9. Users may be responsible for any losses sustained by the District or its affiliates, resulting from the account users' intentional misuse of the accounts.
10. Each computer connected to the internet through the District's network will include technology protection measures that filter or block access to material that is obscene, pornographic or harmful to minors as those terms are defined by law.

Prohibited activity includes but is not limited to:

1. Attempting to modify, install, remove or destroy computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on District-owned equipment.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity

Prohibited activity includes but is not limited to: (continued)

2. Use of computers and user IDs for which there is no authorization, or use of user IDs for purpose(s) outside of those for which they have been issued.
3. Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the District.
4. Computer security systems shall not be circumvented or subverted in any manner. Any unauthorized duplication/redistribution of copyrighted or district computer software, hardware, reports, procedure manuals or other materials is prohibited without proper recorded authorization.
5. Use of the network system shall not serve to disrupt the operation of the system by others; system components including hardware, software, property or facilities shall not be destroyed, modified or abused in any way. Examples include: tampering or altering security codes or passwords, hacking, introduction of viruses, altering, dismantling or disfiguring any file data, including without limitation student data, district, school or staff files, and downloading information or messages without authority.
6. Malicious use of the system to develop programs that harass other users, to gain unauthorized access to any computer or computing system, and/or to damage the components of a computer or computing system is prohibited.
7. Users shall not gain or seek information, obtain copies of or modify files or passwords or any other means, to gain unauthorized access to District systems and information.
8. Using any District computer to pursue hacking, internal or external to the District, or attempting to access information that is protected by privacy laws.
9. Accessing, transmitting or downloading computer viruses or other harmful files or programs, or in any way degrading or disrupting any computer system performance.
10. Uses that jeopardize access or lead to unauthorized access into accounts or other computer networks are unacceptable.
11. Intentionally altering, damaging, destroying, or modifying any computer network, computer property, computer system, program, or software.
12. Activity prohibited under other district policies concerning staff and student use of computers and electronic communications.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Cybersecurity (continued)

District Rights

The District reserves the right to:

1. Review and monitor, as appropriate, all activity on the network for responsible use consistent with the terms of District policy and administrative regulations.
2. Remove a user's access to the network, with or without notice, at any time the District determines that the user is engaged in unauthorized activity or violating District policy. In addition, further disciplinary or corrective action(s) may be imposed for violations of this and other applicable District policies up to and including termination of employment for staff or appropriate disciplinary sanctions for students.
3. Cooperate fully with law enforcement investigation concerning or relating to any suspected or alleged inappropriate activities on the network or any other electronic media.
4. Disciplinary action, if any, for the students, staff, and other users shall be consistent with the District's policies and procedures. Violations of District policies may be cause for revocation of access privileges, suspension of access to District electronic equipment, other employee or school disciplinary action and/or other appropriate legal or criminal action, including restitution.

The District is not responsible for any claims, losses, damages, costs, or other obligations arising from the unauthorized use of the accounts.