

CYBERSECURITY

The Board of Education (Board) considers all data in the computer systems of the District as District assets. Data shall be handled as confidential information. Any use of this information shall relate only to authorized District use. Data shall not be modified or destroyed without appropriate authorization.

The Board believes there are a range of potential cybersecurity threats facing District schools. These threats are specifically driven by motivations to disrupt school operations, harm or otherwise take advantage of individuals associated with schools, and disable, compromise, and/or re-direct school technology assets.

Information technology vulnerabilities can be exploited by individuals wholly external to schools (the online ‘hacker’), as well as by those internal to/associated with specific schools, including by school staff, students, families, and local community members.

The Board sees cybersecurity as a significant and growing issue. Technology has enhanced record keeping, communication and teaching, but a cyber-attack on a vulnerable technology system can cripple District operations and result in the theft of student, parent and other sensitive information.

The rapid pace of technological change means school Board members must redefine what it means to be a good steward of community trust in a world filled with emerging cyber threats to student data and district operations.

All employees and students, in addition to technology staff, must recognize that they share the responsibility of acting as good stewards of intellectual property, student information and other sensitive data. An effective cybersecurity program and culture requires the full efforts of all District personnel and stakeholder groups.

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.
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.
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)

ADMINISTRATIVE REGULATIONS REGARDING CYBERSECURITY

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. Directors, managers, and principals shall approve the appropriate level of system access for each employee for whom they have responsibility for.
5. 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.
6. Employee system access shall be electronically removed upon the employee's employment separation from the District.
7. All requests for system access will be made to the appropriate administrator or teacher.
8. Users may be responsible for any losses sustained by the District or its affiliates, resulting from the account users' intentional misuse of the accounts.
9. 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.
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.

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.

Effective cybersecurity starts with simple steps and caveats. Here are 10 tips from the National Cyber Security Alliance (www.staysafeonline.info), a Washington, D.C.-based public-private partnership of institutions and technology companies.

1. Use anti-virus software.
2. Don't open e-mails or attachments from unknown sources. Be suspicious of any e-mail attachments that are unexpected, even if they come from a known source.
3. Protect your computer from Internet intruders.
4. Regularly download security updates and patches for operating systems and other software.
5. Use hard-to-guess passwords. Mix upper case, lower case, numbers and other characters not easily found in the dictionary. Make sure your password is at least eight characters long.
6. Back-up your computer data on disks or CDs regularly.
7. Don't share access to your computer with strangers. Learn about file-sharing risks.
8. Disconnect from the Internet when not in use.
9. Check your security on a regular basis.
10. Make sure all employees know what to do if a computer or system is believed to be infected or corrupted.

1. Students and Staff

- a. Have each user's passwords follow strict creation policies, such as mandating a password contain a minimum of eight characters, upper and lower case letters, at least one number and a special character. The password should not contain the user's name or username and refrain from using a birthdate or easy to guess words as a password.
- b. Passwords should be set to expire on a regular basis, and users shouldn't be able to reuse a previous password.
- c. Students and staff should log out of the computer every time they are finished with their work to prevent others using their accounts and accessing the network under someone else's name.
- d. Users are not to share passwords with any other faculty member, teacher or students. If it is believed someone else has an individual's password, it should be promptly changed and the network administrator notified.

- e. Users should not click on any link or file in an unknown email, even if the email recipient knows the sender, if that person usually doesn't send attachments. It is worthwhile to contact him/her to confirm that the message and the attachment are authentic.

2. Network Administrators

- a. Do not allow students or staff to install any programs on their computers. An administrative password should be required for any installations and administrators should regulate what can be installed.
- b. Install an up-to-date firewall that provides live updates from the vendor.
- c. Separate the student network from the administrative network so no one from the student network can access the administrative network. Ensure firewall rules are in place to prevent this.
- d. Enforce the password policy mentioned above and create another policy regarding the prompt removal of accounts for staff or students who have left the school.
- e. Any wireless access given to students should require the use of their individual network logins and not a shared password that is used by anyone.
- f. Any guest access to wireless should only allow access to the Internet, and not any other segment of the network. If a shared password is used for this, it should be changed on a regular basis.
- g. Ensure all servers have the latest anti-virus and malware detection software installed.
- h. The email server must have specific anti-virus and spam filtering installed. It must not only scan incoming email, but also email between internal personnel and students.
- i. File permissions should be set to read-only for any staff member who does not need to modify a file on a particular shared drive, and they should not have access to any irrelevant files at all.
- j. Ensure all files, databases, and if possible, any virtual servers, are replicated off site with a reputable cloud provider on a regular basis.
- k. Make sure any servers, devices, and software are regularly updated, and any critical patches applied promptly.
- l. Upgrade any operating systems that are no longer supported by the vendor, as they probably will stop releasing security updates for them.
- m. Third-party vendors should be given access to the system only as needed, and that access should be disabled as it is no longer needed.