P6141.326(a)

An optional policy to consider. This updated model policy incorporates the 2025 updated statutes and anticipates the need to Transition to Phone-Free Schools and stricter age verification requirements.

Instruction

Internet/Computer Networks Use

Online Social Networking

I. Philosophy and Purpose

The Internet and electronic communications have vast potential to support curriculum and student learning~~,~~ and prepare students to become responsible digital citizens. The _____ Board of Education (Board) believes that they should be used in schools as a learning resource, both to develop student skills and to provide ongoing professional development for staff. Accordingly, ~~T~~the District shall provide access to digital resources primarily for instructional purposes – defined as activities directly aligned with curriculum, research, or career development.

The _____ Board ~~of Education~~ further recognizes that the Internet and electronic communications include social media, and that while social media can enhance learning, its unregulated use contributes to social media addiction, mental health risks, and significant instructional distraction. ~~The District shall provide access to digital resources primarily for instructional purposes – defined as activities directly aligned with curriculum, research, or career development.~~

II. Restriction on Personal Devices (Anticipating Adoption of Statewide Ban)

To ensure a distraction-free learning environment and curb social media addiction, the following restrictions apply during the school day:

- **Access Restriction:** Students are prohibited from accessing personal social media accounts via District-provided internet, technology, and devices, or personal ~~"wireless communication devices"~~technology and devices during ~~instructional time~~the school day or school-sponsored activities.
- **Storage Mandate:** All personal ~~wireless~~ technology and devices must be powered off and stored in a (locker/designated classroom area) during the school day, unless explicitly authorized for a specific instructional activity or required by a student's IEP or Section 504 plan.
- **Emergency Protocol:** The District shall maintain a secondary communication protocol for parents to contact students in the event of an emergency, bypassing the need for personal social media or cell phone access.

III. Privacy and Mental Health Protections

In accordance with Connecticut's 2025-26 digital safety standards, all platforms and "social" tools utilized by the District shall meet the following requirements:

- Default Privacy Standards: Any platform approved for student use must default to the highest privacy settings, specifically disabling unsolicited direct messaging from non-commercial adults.
- Prohibition of Addictive Design: The District shall not require or encourage the use of any social media platform that utilizes "addictive features" – such as

Commented [KM1]: Note: The relevant legislation proposed during the 2026 legislative session did not pass as of the adjournment of the session on May 6, 2026.

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

infinite scrolls or engagement-based recommendation algorithms – without a prior Data Protection Assessment and explicit parental consent.

RECEIVED

By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

Instruction

Internet/Computer Networks Use

Online Social Networking

III. Privacy and Mental Health Protections (continued)

- Educational LMS Exemption: Secure Learning Management Systems (e.g., Google Classroom, Canvas) are exempt from these prohibitions provided they are managed by District personnel and do not contain public-facing social networking features.

IV. Data Privacy and Third-Party Tools

Any third-party social or digital tool that captures student-generated content must be vetted through the Connecticut Educational Software Hub. Providers must sign the Connecticut Student Privacy Pledge and confirm that no student data will be used for targeted advertising or to build "behavioral profiles" for non-educational purposes.

V. Reporting and "Online Safety Centers"

The District shall provide annual training to students and staff on utilizing platform-specific Online Safety Centers to report:

- Cyberbullying and harassment
- Unauthorized disclosure of personal information
- Attempts by "unconnected" adults to initiate contact

Among the uses of District-provided internet, technology, and devices at any time, or personal technology and devices during the school day or school-sponsored activities that are considered irresponsible, and which may constitute a violation of this policy, include but are not limited to the following:

1. Uses that violate the law or encourage others to violate the law. This includes ~~the transmittal of offensive or harassing messages~~ harassment; offering for sale or use any substance the possession or use of which is prohibited by District policy; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.

2. Uses that cause harm or threaten to cause harm to others or damage to their property. This includes threats of violence; cyberbullying, including electronic harassment that creates a hostile school environment for the targeted individual; defamation (harming another's reputation by lies); defamation (harming another's reputation by lies); acts of intimidation; employment of another's password or some other user identifier that misleads message recipients into believing that someone else is communicating or otherwise using his/her access to the network or the Internet (i.e., impersonation of another person); uploading a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; participation in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.

3. Uses that jeopardize the security of student access and of the computer network or

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

other networks on the Internet. For example, disclosing or sharing personal passwords with others, or impersonating another user.

~~3.~~4. Use of AI-generated content, deepfakes, or anonymized accounts to target others.

~~4.~~5. Uses that are commercial transactions. Students and other users are not permitted to sell or buy anything over the Internet using District-provided internet, technology, and devices at any time, or personal technology and devices during the school day or school-sponsored activities. Private information shall not be shared.

The foregoing uses may also constitute a violation of this policy while using personal technology and devices outside the school day and school-sponsored activities if the use is disruptive of the educational process or endangers persons or property in accord with Section VI of this policy. Anything set forth in this policy regarding technology and device use during the school day applies equally to students participating in virtual or remote learning environments and for conduct occurring within District-hosted virtual learning platforms.

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

Instruction

Internet/Computer Networks Use

Online Social Networking (continued)

The District shall not be responsible for information/comments posted by students on social media websites ~~when the student is not engaged in District activities and not using District equipment~~.

The District reserves the right to monitor, inspect, copy, review, and store, at any time and without prior notice, all usage of the District's computer network and Internet access, as well as all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the ~~School~~ District, and no user shall have any expectation of privacy regarding such materials.

VI. Personal Technology and Device Use Outside the School Day or Off-Campus

The Board may impose disciplinary consequences for use of personal technology and devices outside the school day or that occurs off-campus when such activity is seriously disruptive of the educational process or endangers persons or property. Among the uses of personal technology and devices outside the school day or off-campus which may constitute a violation of this policy and be subject to discipline include, but are not limited to, the following:

1. Uses that violate the law or encourage others to violate the law. This includes harassment; offering for sale or use any substance the possession or use of which is prohibited by District policy; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.
2. Uses that cause harm or threaten to cause harm to others or damage to their property. This includes threats of violence; cyberbullying, including electronic harassment that creates a hostile school environment for the targeted individual; defamation (harming another's reputation by lies); acts of intimidation; employment of another's password or some other user identifier that misleads message recipients into believing that someone else is communicating or otherwise using his/her access to the network or the Internet (i.e., impersonation of another person); uploading a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; participation in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
3. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, disclosing or sharing personal passwords with others, or impersonating another user.
4. Use of AI-generated content, deepfakes, or anonymized accounts to target others.

This policy shall be interpreted consistent with applicable law, and therefore, does not purport to regulate all student speech outside of the school day. The District acknowledges that students retain certain First Amendment protections outside the school environment and that parents/guardians bear primary responsibility for supervising their

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

children's off-campus conduct.

(cf. 5114 – Suspension and Expulsion/Due Process)

(cf. 5131.8 – Off School Grounds Misconduct)

(cf. 5131.81 – Electronic Devices)

(cf. 5131.911 – Connecticut School Climate Policy)

(cf. 5131.913 – Cyberbullying)

(cf. 5131.42 – Virtual/Remote Learning Code of Conduct)

(cf. 6141.321 – ~~Computer Responsible Use Policy~~Telecommunications/Internet: Acceptable Use)

(cf. 6141.323 – Internet Acceptable Use: Filtering)

(cf. 6141.3291 – One-to-One Device Program)

Legal Reference: Connecticut General Statutes

~~119~~1-210(b)(11) Access to public records. Exempt records.
10-15b Access of parent or guardian~~s~~ to student's records.
Inspection and subpoena of school or student records.
10-233a to 10-233f (Student discipline).
10-234-aa to 10-234dd ~~Definitions. Duties re unauthorized or acquisition of student data.~~(Student Data Privacy Act).
11-8a Retention, destruction and transfer of documents. Centralized microcopying services.
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.
46b-56 ~~(e)~~(g) Access to ~~R~~records of ~~Minors.~~minor child by noncustodial parent.

Federal

Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93568, codified at 20 U.S.C. 1232g.) (FERPA).
Dept. of Education. 34 CFR~~.~~ Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g) parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Children's Internet Protection Act of 2000 (HR 4577, P.L.106554)(CIPA)
Communications Act of 1934, as amended (47 U.S.C. 254[h],[I])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.
Reno v. ACLU, 521 U.S. 844 (1997)
Ginsberg v. New York, 390 U.S. 629, at 642, n.10 (1968)
Board of Education v. Pico, 457 U.S. 868 (1988)
Hazelwood School District v. Kuhlmeier, 484 U.S. 620~~, 267~~ (1988)
Mahanoy Area School District v. B.L., 594 U.S. 180 (2021)[C3.1]
Wisniewski v. Bd. of Educ., 494 F.3d 34 (2d Cir. 2007)
Doninger v. Niehoff, 642 F.3d 334 (2d Cir. 2011)
~~Public Act 24-141, An Act Concerning Social Media Platforms and Minors~~
Public Act 25-113, An Act Concerning Broadband Internet, Gaming, Social Media, Online Services and Consumer Contracts

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

Policy adopted:
rev 9/25

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

rev 4/26

RECEIVED

By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

CABE POLICY SERVICES

R6141.326(a)

This model administrative regulation provides the procedural framework to implement the 2026 updated board policy 6141.326.

Instruction

Internet/Computer Networks Use

Online Social Networking

I. Instructional Purpose and Vetting: To ensure that all social media use is "primarily for instructional purposes," the following vetting process is established:

- Prior to utilizing any third-party digital tool or social platform with students, staff must verify its status on the Connecticut Educational Software Hub.
- If a tool is not on the Hub, the District Technology Coordinator must obtain a signed Connecticut Student Data Privacy Pledge from the provider, ensuring compliance with C.G.S. §§ 10-234aa to 10-234dd.
- Teachers must include the specific learning objective (e.g., "collaborative research," "digital citizenship") in their lessons when a social networking component is required.

II. Device Management and Storage: (In anticipation of HB 5035-2026's legislative session mandates, schools will implement the following personal device restriction procedures:

- **The "School Day" Window:** Defined as the period from the first bell to the final dismissal bell.
- **Storage Protocols (Middle School/High School):** Devices must be stored in lockers or (secure classroom pouches).
  - **Elementary Schools:** Devices must remain in backpacks and powered off.
- **Authorized Use Exception:** A teacher may authorize a "one-time instructional bypass" for a specific activity requiring the use of a personal electronic device. In such cases, devices are returned to storage immediately upon completion of the learning activity.
- **IEP/504 Carve Out:** Students with documented medical or educational needs (e.g., glucose monitoring, assistive communication) are exempt from storage mandates as outlined in their specific approved plan.

III. Emergency Communication Protocol: To bypass student reliance on personal devices during emergencies:

- Centralized Messaging: Parents shall be directed to use the (District Notification System, e.g., ParentSquare) for all urgent updates.
- Classroom Access: Every instructional space must maintain a functioning landline or internal VOIP system for immediate administrative contact.
- (Other considerations should be determined by the District's School Security and Safety Committees and included in the School Security and Safety Plans)

Commented [KM2]: Note: This legislation proposed during the 2026 legislative session did not pass as of the adjournment of the session on May 6, 2026.

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

Instruction

Internet/Computer Networks Use

Online Social Networking (continued)

IV. Digital Safety and "Addictive Feature" Compliance: Administrators or their designees shall conduct an annual audit of District-sanctioned platforms to ensure:

- Settings are verified to "Private" by default. Unsolicited direct messaging from non-connected accounts ~~are~~ is required to be blocked.
- For any platform using a recommendation algorithm (e.g., YouTube for Schools), the District shall provide parents with a Digital Disclosure Notice at the start of the year, allowing for an "Opt-Out" of algorithmic content.
- Building administrators will ensure that "public-facing" features, such as public comments or open profile discovery, are disabled within the District's Secure Learning Management Systems (e.g., the Google Classroom/Canvas environment).

V. Annual Training and Incident Reporting:

- The "Online Safety Center" training shall be integrated into the Grade 6-12 Health or Advisory curriculum.
- Violations, including but not limited to Cyberbullying and Harassment, must be reported via the District's Title IX/Bullying Reporting Portal.
- Staff are required to assist students in utilizing the "Report" function within specific social media platforms when "unconnected adults" attempt contact.

VI. Enforcement and Sanctions: Violations of this regulation, including "hacking," unauthorized device use, or bypassing district filters, will result in disciplinary action as outlined in the Student Code of Conduct, which may include:

- Temporary confiscation of the device (returned only to a parent/guardian).
- Revocation of District network privileges.
- Suspension/expulsion for severe infractions ~~(e.g., uploading viruses or cyberbullying)~~.

VII. General Expectations: The use of permitted social networking sites by students on District computers shall conform to the following guidelines:

- The search for illegal, crude, crass, and inappropriate things is not acceptable and should be avoided.
- Computers and accessing social media sites should be used for research and school projects or to connect with other students in a responsible manner.
- Social networking sites should not be used to harass other students.

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026

Instruction

Internet/Computer Networks Use

Online Social Networking

VII. General Expectations: The use of permitted social networking sites by students on District computers shall conform to the following guidelines: (continued)

- Be mindful of copyright infringement, plagiarism, illegal downloading, and AI-generated content.
- Utilize teachers and administrators to determine if the site to be used is appropriate.
- Leave an inappropriate site immediately and notify available staff.
- Assignments involving the use of social networking tools on the Internet are like any other school assignment, subject to the Board's policies, the District's regulations, and rules and procedures in the student handbook.
- Online social networking and the frequent use of Internet sites that contain personal information also increase the opportunity for unwelcome and unsolicited written material, pictures, or videos. Harassment in any form, including electronically posted comments, is unacceptable.

RECEIVED
By Marc J. Garofalo, MPA, MCC, MCTC at 2:46 pm, May 11, 2026