

SECTION IX - TECHNOLOGY SAFETY AND ACCEPTABLE USE⁸⁹

Content Filtering and Technology Monitoring⁹⁰

Students have no right or expectation to privacy when using District information and technology resources. The District utilizes technology tools to filter and monitor online activity of students using District-owned/operated devices and networks.

Content Filtering

Filter technology protects against access to content that is inappropriate for and/or harmful to students as defined by the Children's Internet Protection Act (CIPA). The District may further filter content to ensure smooth, uninterrupted operation of the network and adequate technology resources (e.g. Internet bandwidth) are at all times available for the District's educational and operational purposes and to support the educational use of technology through classroom management.

However, because the Internet is a constantly-changing public gateway, parents/guardians and students are advised that it is not always possible to technologically limit access to only the services authorized by District staff. It is impossible to guarantee students will not gain access through the Internet to content that they and/or their parents may find inappropriate, offensive, objectionable, or controversial. Parents/Guardians should set and convey standards for use of the Internet at home.

Monitoring

The District may monitor student technology (e.g. devices, accounts, messages) for purposes of student safety, classroom management, compliance with Acceptable Use, recovery of a lost or stolen device, and IT management or troubleshooting. Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions or use of specific monitoring tools to review browser history and network, server, and computer logs. Monitoring is in accordance with Ohio Revised Code.

District access to student technology may prompt notification to parents/guardians within seventy-two (72) hours of such access, explaining the circumstances prompting the access, what features were accessed, and a description of any related threat. Should notification itself present or exacerbate a threat, notification is not required at any time.

Disabling or Bypassing

Filtering and monitoring tools are used both to keep students safe and to comply with federal and state laws and District policies. Disabling, bypassing, or attempting to disable/bypass any safety or security measures on District-owned/operated technology, including use of proxies or VPNs, is prohibited and subject to discipline.

⁸⁹ Board Policies [7540 - Computer Technology and Networks](#), [7540.01 - Technology Privacy](#), [7540.02 - Web Accessibility, Content, Apps, and Services](#), and [7540.03 - Student Technology Acceptable Use and Safety](#)

⁹⁰ Board Policy [5136.01 - Electronic Equipment](#) and [7540.03 - Student Technology Acceptable Use and Safety](#)

District Device Use/1-to-1 Chromebook Program

The District provides students access to technology resources required to successfully complete its programs. Students should use District-owned/operated technology for school-related work, both on- and off-campus.

District-Issued Email Account⁹¹

All students are issued a Google Workspace for Education account (“username”) for all school-related electronic communication and for signing up, registering, or accessing various school-related online platforms or apps.

Sending or forwarding bulk or mass emails (i.e. to an excessive number of recipients) or using the District-issued account to distribute unauthorized material is prohibited.

Chromebook and Account Assignment

Grades K-4

Through fourth grade, students use Chromebooks from charging carts located in or near each classroom. Teachers may assign a specific device to each student to monitor proper use. Under special circumstances authorized by the Principal (e.g. extended medical leave) devices may be issued for take-home use.

Students may sign-in with a QR code associated with their assigned username.

Grades 5-8

Fifth grade students are assigned a Chromebook with a protective case and one (1) charger for use through eighth grade. Devices are primarily used and kept at school but may be sent home at the discretion of teachers or the Principal. The device is returned at the conclusion of eighth grade.

Beginning in fifth grade, students sign-in with an assigned username and password.

Grades 9-12

Ninth grade students are assigned a new Chromebook with a protective case and one (1) charger for use through graduation. Students maintain possession of their device at all times and are solely and at all times responsible for its use and care, both on- and off-campus. Graduates may be invited to keep their device.

Students may be able to personalize their account passwords for security purposes.

New/Returning Students

Newly-enrolled students will receive a Chromebook model most closely aligned with those of their graduating class. Students enrolling late in the Chromebook cycle (e.g, 8th or 12th grade) may receive a refurbished device.

Students returning to/re-enrolling in the District may not receive the device originally issued to them, but will receive a comparable model.

⁹¹ Board Policy [7540.06 - District-Issued E-Mail Account](#)

Getting Help and Support

Any Chromebook, charger, or case that is broken or fails to work properly must be taken to the help desk in the building for an evaluation of the equipment. The location of the help desk in each building will be communicated at the start of the school year.

Do not disassemble or attempt to repair the Chromebook or accessories. The Chromebook will be repaired or replaced as quickly as possible.

A loaner device may be provided at the discretion of the school. Delays may occur if building administrators must investigate disciplinary issues surrounding any damage.

Property and Release

These devices are and remain the property of the District until and unless they are released to students in specific circumstances (e.g. graduation).

Check-In/Turn-In

Students issued a take-home device may be required to check-in (present to staff for identification and inspection) and/or turn-in (return to staff) the device and accessories at any time, but particularly at the conclusion of a school year. Failure to check-in or turn-in may result in a fee for the full replacement cost of the device.

Students may be permitted to retain devices during summer break at the discretion of the Principal. This policy will continue to apply.

Student Withdrawal

If a student transfers out of the district, the device, charger, and case must be returned to the student's school office at the time of withdrawal. Families who do not return the device and accessories will be invoiced. Students who are expelled or terminate enrollment in the Newark City School District for any other reason must also return the school device, charger, and case on the date of termination.

Proper Use and Care

Students are at all times responsible for the care and proper use of the device, charger, and case.

Student Sole Use

- The Chromebook and accessories are provided for the sole use of the student to whom they are assigned.
- Students may not lend or permit access to their device, charger, cable, case, or any other accessories to other individuals.

Exterior and Case

- Chromebooks are issued with a protective case and must be transported and used in the case issued. If the case is removed, altered, or replaced, any protection plan will be void and families will be responsible for the full cost of the case and device if damaged or lost.

- Identification tags placed under or on the device or its protective case may not be removed or tampered with. If a tag becomes loose, damaged, or falls off, the device should be presented to staff for a new tag.
- If the case is damaged intentionally or through negligence, a \$35 replacement fee may apply.
- Use only a soft, dry, lint-free microfiber cloth to clean the screen. A small amount of window cleaner or alcohol applied on such a cloth may be used to clean the plastic device exterior. Never spray cleaners directly onto the device. Do not use household cleaners, aerosol sprays, solvents, ammonia, or abrasives to clean the device.

Home/School Transportation

- Students transporting Chromebooks between home and school are responsible for bringing the device to school fully charged each day.
- It is expected that the case be closed during transportation and times when it is not in use.

Personalization

- Do not write/draw on, deface, apply stickers, or otherwise alter the appearance of the device or accessories. This makes it impossible to re-issue the device to another student and may subject the student to replacement fees.
- Students may install approved Chrome extensions and ChromeOS apps. Students should make use of Google Drive for all files. Data saved to the Chromebook (e.g. in “Downloads”) is temporary, not part of Google Drive, and will be lost in the event of device replacement or software reset.
- Students may not jailbreak, modify, or in any other way tamper with the Chromebook software.
- Chromebooks must remain connected to the pre-assigned wireless network when on-campus. They are capable of connecting to any modern consumer WiFi network off-campus.

Chargers

- Chargers should be used only for the assigned-student’s Chromebook and not loaned to others or used to charge other devices.
- Chargers have delicate cables prone to damage from mishandling (e.g. winding too tightly) or negligence (e.g. from pets).

Audio

- Sound must be muted unless permission is obtained from the teacher for instructional purposes.
- Earbuds/headphones may be used in the classroom with teacher approval.
- Earbuds/headphones are the responsibility of the student.

Damage Avoidance Tips

- Avoid leaning on the Chromebook or placing anything on top of it. Placing too many items in a carrying case or backpack may put too much pressure on the device and cause irreparable damage to the screen, plastics, or internal electronics.
- The device must not be used or stored near food or drink.
- Keep the device out of extreme temperatures, away from hot/cold surfaces, and away from water or dampness. Excessive environmental conditions will damage components and impact battery life.
- Keep the device and accessories inaccessible to pets and off the floor where they could be stepped on or tripped over.
- Make sure the case cover is secured over the device when not in use.

Device Protection Plan

- Problems affecting the device's functionality that are determined to be manufacturing flaws and minor unintentional damage will be covered by the District at no cost to students.
- Cosmetic issues and normal wear-and-tear not affecting the device's functionality are expected and not subject to repair or device replacement.
- Devices issued starting Fall, 2025 have a comprehensive protection plan for four (4) years from District purchase (NOT from issuance to the student). Older devices may be covered at the District's discretion at the District's expense.
- Cases are not covered by the protection plan and are subject to replacement with a fee.

Negligence, Misuse, and Intentional Damage

Intentional or severe damage may incur fees, up to the full replacement cost (currently \$400). Assessed repair fees will reflect the actual cost to the District of parts and labor. The determination of intentional, negligent, or accidental damage and whether to assess a repair fee is made by the Principal with input from the repair team.

Vandalism, damage, or loss caused by another student is subject to discipline and fees may be assessed to the account of the vandal.

Repeated offenses may result in the revocation of a student's 1-to-1/Chromebook privileges. Devices will be provided under monitored conditions as needed for classwork and testing.

Theft

Theft is not covered by the device protection plan.

In the event of theft, parents/guardians or adult students must immediately file a police report in the jurisdiction where the theft took place and provide a copy to the Principal for investigation and consideration of a replacement fee waiver.

Chromebooks must never be left in an unlocked locker, unlocked car, or any unsupervised area or bag. Such occurrences would be deemed as negligence. If the theft is due to negligence, a full replacement fee may be assessed. Any fee waiver is at the discretion of the District on a case-by-case basis.

Device location and usage may be tracked for purposes of retrieving lost or stolen devices. Missing or suspected-missing devices may be placed in a lockdown mode.

Technology Fee

The technology fee of \$40 partially sustains the purchase and maintenance requirements of the 1-to-1 program. This fee is waived in specific circumstances in accordance with District policy and state law.

Personal Communication Devices⁹²

The District provides students with access to technology resources required to successfully complete its programs. **Use of non-District-owned/operated technology is restricted. Students should use District-owned/operated technology for school-related work, both on- and off-campus.**

Use of personal communication devices ("PCDs") is limited during school hours and during school-related events. Examples of PCDs include computers, laptops, tablets, e-readers, cellular telephones, smartphones, gaming devices, smartwatches and other wearable technology, and other web-enabled devices used to communicate.

Students are personally and solely responsible for the care and security of their PCDs. The District assumes no responsibility for theft, loss, or damage to, or misuse or unauthorized use of, PCDs.

When the use of PCDs is prohibited, all PCDs must be powered off completely (i.e., not just placed in vibrate or silent mode) and stored out of sight.

During the school day, parents/guardians should call their student's school office to reach them and, with permission from staff, students may use school phones to contact parents/guardians.⁹³

Permitted PCD Use

Nothing in this policy prohibits a student from using a PCD for student learning or to monitor or address a health concern, in accordance with the student's individualized education program or Section 504 plan.

Further exceptions for PCD use for educational purposes may be authorized by the Principal. Exceptions during non-academic periods of the school day (e.g. lunch, passing time, study hall) are at the discretion of the Principal.

When the use of PCDs is permitted, all PCDs must be placed in silent mode and must be stored out of sight when directed by the administrator or a teacher.

⁹² Board Policies [5136 - Personal Communication Devices](#), [5136.01 - Electronic Equipment](#), and [7542 - Access to District Technology Resources and/or Information Resources from Personal Communication Devices](#)

⁹³ Handbook Section ["Use of Office Telephones"](#)

Use of non-District-owned/operated PCDs is subject to the same policies and laws applied to use of District-owned/operated devices.

PCD Network Access and Security⁹⁴

To minimize the District's exposure to potential damage, connections to the District's network from PCDs are limited to "Guest" or "BYOD" ("Bring Your Own Device") networks. Such networks require authentication and are restricted to Internet access only. Students may not use non-District-owned/operated PCDs to access other District technology resources without authorization from the Technology Director. PCD network connections are not guaranteed and may be disabled or access revoked at any time.

Students may not use PCDs to access and/or view Internet websites that otherwise are blocked to students while in school, on school property.

Any attempt to access, alter, or disrupt District technology resources, or to access the technology of other users, through use of a PCD is prohibited.

Privacy⁹⁵

Students have no expectation of confidentiality with respect to their use of PCDs while at school or on school property, including school buildings, other facilities, and school vehicles, or when using any District-owned/operated technology resources.

Students may not use devices to infringe on another person's reasonable expectation of privacy. This includes using devices in locations and circumstances where a student may be changing clothes or in any stage of undress, such as gymnasiums, locker rooms, shower facilities, and restrooms/bathrooms, and swimming pools. The Superintendent and Principal may determine other locations and situations where the use of a device is absolutely prohibited.

Except as authorized by a teacher, administrator, IEP team, or Section 504 plan, students are prohibited from using devices to capture, record, and/or transmit the words or sounds (i.e. audio) and/or images (i.e. pictures/video) of any student, staff member, or other person during school hours on school property. Using a device to capture, record, and/or transmit audio and/or pictures/video of an individual without proper consent is considered an invasion of privacy, is not permitted, and is subject to disciplinary action according to the Student Code of Conduct.

Students are expressly prohibited from using covert means to listen-in or make a recording (audio or video) of any meeting or activity at school. This includes placing recording devices, or other devices with one- or two-way audio communication technology, within a student's book bag or on the student's person without express written consent of the Superintendent.

The Principal has authority to make determinations as to other specific locations and situations where possession of a camera or other electronic equipment/device is absolutely prohibited.

⁹⁴ Board Policy [7542 - Access to District Technology Resources and/or Information Resources from Personal Communication Devices](#)

⁹⁵ Board Policy [5136.01 - Electronic Equipment](#)

Reporting Requirement

Knowledge of a student using a PCD, recording device, or other device with one- or two-way audio communication technology in violation of this policy must be reported to the Principal.

Cyberbullying/Cyber Harassment⁹⁶

Students may not use technology in any way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated. In particular, students are prohibited from:

- A. transmitting material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, color, national origin, sex (including sexual orientation/transgender identity), disability, age, religion, ancestry, or political beliefs; and
- B. engaging in "sexting" - i.e., sending, receiving, sharing, viewing, or possessing pictures, text messages, e-mails or other materials of a sexual nature in electronic or any other form.

Violation of these prohibitions will result in disciplinary action and be reported to local law enforcement and child services as required by law.

Technology and Academic Integrity⁹⁷

Students may not use devices to capture, record, and/or transmit test information or any other information in a manner constituting fraud, theft, cheating, or academic dishonesty. Likewise, students are prohibited from receiving such information. Staff may require students to remove wearable PCDs, such as smartwatches and smart glasses, to ensure academic integrity.

Use of Artificial Intelligence (AI)⁹⁸

When AI tools are used responsibly and effectively, they can supplement, not replace, the learning and problem-solving skills that are essential to success. Misuse of these technologies undermines the integrity of the educational process.

If a student has questions about whether they are permitted to use AI tools for a specific class assignment, they should ask their teacher.

Authorized Use

Students may use AI tools for classwork only with permission/consent from their teacher. Teachers have the discretion to authorize students to use AI tools for the following uses:

- A. Research assistance

⁹⁶ Board Policies [5517.01 - Bullying and Other Forms of Aggressive Behavior](#) and [5136.01 - Electronic Equipment](#)

⁹⁷ Board Policy [5136.01 - Electronic Equipment](#)

⁹⁸ Board Policies [7540.03 - Student Technology Acceptable Use and Safety](#) and [7540.09 - Artificial Intelligence](#)

- B. Data analysis
- C. Language translation
- D. Writing assistance
- E. Accessibility

Attribution of AI-Generated Content

In accordance with their teacher's direction, students are required to cite/identify work generated/created with the use of AI tools and explain/demonstrate how the AI tools were used in the creation of the work.

Unauthorized use of AI tools is considered a form of plagiarism and subject students to discipline.

Confiscation and Search⁹⁹

Unauthorized electronic equipment and devices used inappropriately will be confiscated from the student by school personnel and disciplinary action taken.

Any electronic equipment/device confiscated by District staff will be marked in a removable manner with the student's name and held in a secure location. School administrators may choose to release devices only to parents/guardians.

School officials will not search or otherwise tamper with PCDs in District custody unless they reasonably suspect that the search is required to discover evidence of a violation of the law or other school rules.

Enforcement

Use of technology in violation of this policy can result in temporary or permanent loss of network and Internet access, loss of 1-to-1 Chromebook privileges, and/or disciplinary action.

Network and Internet access for student-owned PCDs during school hours and during school-related events and functions is a privilege that may be forfeited by any student who fails to abide by the terms of this policy, or otherwise abuses this privilege.

Students are responsible for the costs of repairs to District-owned/operated technology that is damaged intentionally, stolen, or lost.

If a violation involves an illegal activity (e.g. child pornography, sexting), the school official will also refer the matter to law enforcement or child services. Devices will be confiscated and may be turned over to law enforcement if a violation involves potentially illegal activity.

⁹⁹ Board Policies [5136.01 - Electronic Equipment](#) and [5771 - Search and Seizure](#)