



Book	East Islip School District School Board Policies
Section	Policy Nos. 4327-4830
Title	Computer Network and Internet Access Acceptable Use
Code	4526
Status	Active
Adopted	June 8, 1999
Last Revised	December 12, 2024
Prior Revised Dates	04/11/2019

4526

COMPUTER NETWORK AND INTERNET ACCESS ACCEPTABLE USE

The Board of Education is committed to the optimization of student learning and teaching. The Board of Education considers a computer network, including the internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in School District classrooms for the purpose of advancing and promoting learning and teaching.

Within financial limitations, computers, computer networks and the internet will be made available to students, faculty and staff. The technology resources at the School District (e.g., all networking, hardware and software, the Internet, e-mail, telephone equipment, digital still and video, voice mail, fax machines and supporting telephone lines, and all communication equipment) are provided to support the educational and administrative activities of the School District and should be used for those purposes. An individual's use of the School District's computer resources must be in support of education and research and consistent with the educational objectives of the School District.

The computer network can provide a forum for learning various software applications and, through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communications opportunities for staff and students.

When an individual accesses computers, computer systems and/or computer networks, including the internet (hereinafter the "School District's computer resources") provided by the School District, he/she assumes certain responsibilities and obligations. Access to the School District's computers, computer systems and/or computer networks is subject to federal, state and local law, as well as Board of Education policy. The use of the School District's computers, computer networks and the internet is a privilege, not a right, and inappropriate use will result in the cancellation of privileges and/or disciplinary action by School District officials.

All users of the School District's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The School District reserves the right to control access to the Internet for all users of its computers and network. The School District may either allow or prohibit certain kinds of online activity, or access to specific websites.

The Board of Education directs the Superintendent of Schools to designate a computer coordinator to oversee the use of School District computer resources. The computer coordinator will prepare in-service programs for the training and development of School District staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

Definition of Terms

The School District's computer network refers to the interconnection of computers, servers, and other electronic devices within a classroom, school, or School District which facilitates file sharing, resource sharing, communication, collaboration, management, and access to remote resources.

The Internet is a decentralized network of computer networks, which provides connectivity to commercial, educational, organizational and government resources and facilitates local and global communication.

For purposes of this policy, the definition of public social media networks or social networking sites (SNS) are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites, and any other social media generally available to the School District community which do not fall within the School District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, TikTok, Discord, BeReal, WeChat, WhatsApp, blog sites, or any other social media platforms). Employees are required to maintain the highest level of professionalism when communicating in their professional capacity as educators. Employees have a responsibility to address inappropriate behavior or activity on these networks, including compliance with all applicable School District policies and regulations.

The Board of Education recognizes that for any School District employee, the contents of electronic communications, including email, instant messaging, listservs, blogs, wikis, social networking sites (Facebook, LinkedIn, Twitter, Instagram, etc.), should be composed with the utmost care. Because many of these tools occupy online public spaces, the potential to bring harm to oneself, to others, and to the School District must be recognized, as recipients may forward messages to locations where there is no control over future dissemination.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Executive Director for Student Achievement and Instructional Technology. The Executive Director for Student Achievement and Instructional Technology will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

Authorized Use

Authorized users of the School District's computer resources include members of the Board of Education, administrators, supervisors, faculty, staff, students, parent/persons in parental relation and any other person who has been granted access to the School District's computer resources. Unauthorized use is strictly prohibited. By utilizing the School District's computer resources or personally-owned equipment, the user consents to the School District's exercise of its authority and rights as set forth in this Policy with respect to the School District's computer resources, as well as with respect to any information or communication stored or transmitted over the School District's computer resources.

Faculty, staff members, and students (where applicable) may be provided with e-mail accounts and Internet access. Whenever a user ceases being a member of the School District community or if such user is assigned a new position and/or responsibilities, use of the School District's computer resources for which he or she is not authorized in his or her new position or circumstances shall cease and property returned. When a School District employee separates from service from the School District, access to all School District accounts and email is disabled. All School District business being conducted electronically must be performed with a School District account or service. Employees should not use private email accounts. Email used for School District purposes may be subject to FOIL. There is no expectation of privacy when utilizing School District email.

Use of Personal Electronic Devices During the School Day and at School Sponsored Events

Personal electronic devices include, but are not limited to, personal smart devices, and electronics including but not limited to: traditional cell phones and flip phones; wearables such as smart watches; iPhones and Android smartphones; Bark phones and other smartphones with modified application menus and parental controls; iPads and other tablets such as Kindles; personal laptops and other computers; air pods and earbuds, all recording devices, and such other Internet connected devices and handheld devices that are available for use.

All students are required to turn off any/all personal electronic device(s) as defined above and store the personal electronic device(s) in their backpack or school-provided locker for the duration of the entire school day between the hours of the opening bell through dismissal in each school building. The personal electronic device(s) must then remain in the backpack or school-provided locker for the duration of the entire school day between the hours of opening bell through dismissal in each school building. The device(s) must be out of sight and not be on the student's person at any time during the school day or during school sponsored events. The building administration has the discretion to allow students to use personal electronic devices in specific cases, such as medical conditions, educational needs, or other limited situations.

All employees are required to turn off or silence their personal electronic devices during school hours, defined as opening bell through dismissal, so that workflow remains undisturbed.

In addition, employees should make their best effort to stow their personal electronic device(s) in a bag or desk drawer during live classroom instruction so that personal electronic devices are out of the sight of students. The personal electronic device(s) must then remain out of sight during teaching periods, prescribed work hours, or building duties. Personal electronic device(s) can be used during a prep period, break, or lunch break. Personal electronic devices must not be used to take pictures of students or to post photos of students on an employee's social media platform.

Employees, including coaches and club advisors are required to communicate with students concerning assignments and after school activities. through School District approved electronic means.

The School District insists that all employees act responsibly in their jobs so as not to endanger the lives of themselves or others. No telephone communication, business or personal, is so necessary or urgent that it cannot be postponed or interrupted until such time as the involved person can participate in the phone call without compromising safety. Safe driving is always the first responsibility. The School District actively discourages the use of hand-held cellular phones, and other wireless communication devices, while driving cars, trucks and golf carts both on and off campus, during School District work time or on School District business.

Further, employees should not dial, text, email or otherwise violate the law related to the use of electronic devices while driving on School District business. If an employee must engage in any of the above activities, he or she must pull over to a safe location off the roadway and out of

traffic, stop and park the vehicle before doing so. Stopping in a roadway breakdown lane is by its very nature dangerous and therefore is not considered a safe location by the School District.

The School District acknowledges that members of the school administration, members of the facilities department and computer services and athletic trainers often use two way radios and radio-telephones in the School District in the performance of their daily duties. In addition, the use of wireless devices by building administration and security guards are both prevalent and necessary. These employees are reminded to use these devices in such a manner so as not to compromise safety.

Employees may not post photos of students on personal social media accounts.

Employees, including coaches and club advisors, are required to communicate with students concerning assignments and after school activities through School District approved platforms. With the approval of the building principal, employees may post photos of students that have given photo consent on School District approved platforms.

Further, the School District will not be liable for the loss, damage, theft or misuse of any personal electronic device(s) brought to school. The School District will bear no responsibility nor provide technical support, troubleshooting, or repair of electronic devices owned by anyone other than the School District. Students and staff are responsible for understanding and inquiring about the use of technology prior to engaging in such use.

Privacy Expectations

The School District's computer resources, including all telephone and data lines, are the property of the School District. The School District reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the School District's network and it may be required by law to allow third parties to do so. Electronic data, e.g., may become evidence in legal proceedings. In addition, others may inadvertently view messages or data as a result of routine systems maintenance and monitoring or misdelivery.

Users must recognize that there is no guarantee of privacy associated with their use of School District computer resources. Users should not expect that e-mail, voice mail or other information created with or maintained in the School District's computer resources (including the use of Google Drive or a similar application and even those marked "personal" or "confidential") are private, confidential or secure.

Responsible Use

1. All users must not act in ways that invade the privacy of others, are unethical or fail to comply with all legal restrictions regarding the use of electronic data. All users must also recognize and not violate the intellectual property rights of others.
2. All users must maintain the confidentiality of student information in compliance with federal and state law including, but not limited to, FERPA, HIPAA and Education Law, section 2-d.
3. Disclosing and/or gossiping (including but not limited to via e-mail, voice mail, Internet instant messaging, social media, chat rooms or on other types of Web pages) about confidential or proprietary information related to the School District is prohibited.
4. All users must refrain from acts that waste School District computer resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to

tamper with, circumvent filtering or access, or degrade the performance of the School District's computer resources or to deprive authorized users of access to or use of such resources are prohibited.

5. Students may not send broadcast e-mail or broadcast voice mail.

6. Users are responsible for both the content and possible effects of their messages on the network. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying or harassing material), and billable services.

7. Official email communications must be professional, ethical and meet the standards of other School District publications bearing in mind that the writer is acting as a representative of the School District and in furtherance of the School District's educational mission.

8. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in School District email unless used in the furtherance of business of the School District as part of the curriculum of the School District.

9. The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the use of social media tools and the exploration of new and emerging technologies may be used to supplement a student's instructional program.

10. The signature portion of the user's email may not include external links or graphics that are unrelated to the content of the email.

11. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.

12. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used on School District equipment except as permitted by law and approved by the Executive Director for Student Achievement and Instructional Technology or his/her designee in accordance with the procedures established for use of software/hardware with the School District's computer resources. All software license provisions must be strictly adhered to.

13. Students are not permitted to record classroom instruction without the express permission of the teacher.

14. The School District fully supports the experimental educational and business use of digital resources including, but not limited to, software, third party applications, websites, web-based programs and/or any applications/resources which require a login/password and has a Executive Director for Student Achievement and Instructional Technology to support this purpose. Since the installation of digital resources, other than district-owned and district-tested digital resources could damage the School District's computer resources, compromise student data/privacy and/or interfere with others' use, digital resources downloaded from the Internet or obtained elsewhere must be approved by the Executive Director for Student Achievement and Instructional Technology or his/her designee. Digital resources may not be installed onto any district owned or district-leased computer unless in compliance with the Board of Education's policies concerning purchasing and computer resources. Once digital resources have been approved by Executive Director for Student Achievement and Instructional Technology, installation will be scheduled and performed.

Inappropriate Materials

1. The School District prohibits faculty, staff and students from developing, maintaining, and transmitting pornography in any form at school, including, but not limited to, magazines, posters, videos, electronic files or other electronic materials.
2. Accessing the School District's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the School District is prohibited. The School District will respond to complaints of harassing or discriminatory use of the School District's computer resources in accordance with Policy 0100 (Equal Opportunity), Policy 0110 (Sexual Harassment) and/or Policy 0115 (Dignity for All Students Act). These provisions are not intended to prohibit an authorized user from carrying out his or her assigned educational, employment or administrative function.

The person to whom the School District has issued an electronic device will be liable for the loss, damage, theft, or misuse of said electronic device(s) issued by the School District. In addition, a student or staff member will be responsible for the full replacement cost of the device if the loaned device is lost, damaged, stolen or misused.

School District Social Media Platforms

The Board of Education recognizes that social media platforms may be utilized by staff as "content owners" to engage parents, community members, students, and employees. The School District's social media platforms provide a mechanism to share information with the school community concerning various events, accolades, and accomplishments in the School District. In addition, social media platforms may be used to provide information regarding school news, closures, or information to be shared with the school community.

"Social Media" includes the various online technology tools that enable people to communicate and share information over the Internet. Social media can include text, audio, video, images, and other multimedia communications.

School District presence on any social media site, including School District-related accounts, such as clubs, teams, or other sites associated with the School District or a school in the School District must be authorized by the individual designated by the Superintendent of Schools or designee. Any accounts existing prior to this policy's adoption will be subject to review.

For emergency and data collection purposes only, each School District-related site or social media account must name the individual designated by the Superintendent of Schools or designee as an administrator. However, the content owner shall be responsible for monitoring and maintaining these accounts. The School District's primary, official social media platforms will be managed by the individual designated by the Superintendent of Schools. Official School District social media accounts will not participate in advertising, nor promote commercial enterprises. School District social media accounts may share relevant community events and updates as approved by the Superintendent of Schools or his/her designee.

Before posting any student work, photographs/videos, or other personally identifiable information (PII), online or to social media, content creators shall review the child's "Release of Information" status to ensure that the parent/person in parental relation have allowed such content to be published digitally. No student photographs or videos should be published for personal, promotional use or any other non-school related purpose.

Confidentiality and Privacy Rights

Individuals must take all reasonable precautions to prevent unauthorized access to accounts or data by others, both inside and outside the School District. Individuals will not leave any devices unattended with confidential information visible. All devices are required to be locked down when an individual steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Data files and electronic storage areas shall remain School District property, subject to School District control and inspection. The Executive Director for Student Achievement and Instructional Technology or his/her designee may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy.

Security

1. Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School District, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the district's system, the individual consents to the School District's right to do so.
2. Removing School District computer resources from the School District's facilities and/or relocating School District computer resources (not including portable technology devices) requires prior authorization from the Executive Director for Student Achievement and Instructional Technology or his/her designee.
3. Unless approved by the Executive Director for Student Achievement and Instructional Technology or his/her designee, modem use is prohibited on computers that are directly connected to the School District network. Personal network appliances may not be connected to the School District network and may be confiscated.
4. Storage of copyrighted materials such as music, video and games is prohibited.
5. Users may not attempt to circumvent or subvert the security provisions of any other system. Without authorization from the Executive Director for Student Achievement and Instructional Technology or his/her designee, no one may attach a server to or provide server services on the School District network.

The Internet at the School District

1. There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on website, chat rooms or other systems. The School District cannot guarantee that users will not encounter text, pictures or references that are objectionable. Responsible attitudes and appropriate behavior are essential in using this resource. As with e-mail, information that a user places on the Internet is akin to sending a postcard rather than a sealed letter. Its contents may be accessed by system administrators in this School District and elsewhere.
2. Users must be aware that some material circulating on the Internet is copyrighted and subject to all copyright laws. Materials taken from the Internet must be properly cited.
3. Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the School District's system to download illegally distributed material.
4. Users are cautioned not to open e-mail attachments or download any files from unknown sources in order to avoid damaging School District computers and bringing destructive viruses into the School District's system. Anything questionable should be reported immediately to the Executive Director for Student Achievement and Instructional Technology or his/her designee.

5. With permission, students, faculty and staff may create or modify web pages on the School District web servers. To ensure the integrity of these sites, users must abide by the School District's web practices. It is the user's responsibility to update and maintain all links and content, keeping in mind the Inappropriate Materials section and the copyright requirements.

School District Limitation of Liability

The School District does not warrant in any manner, express or implied, that the functions or the services provided by or through the School District system will be error-free or without defect. The School District shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

Users of the School District's computer resources, including internet use, do so at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. Further, even though the School District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the Board of Education and School District policy and regulations.
Policy Enforcement and Sanctions

1. All members of the School District community are expected to assist in the enforcement of this policy. Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer, telephone or network access privileges, disciplinary action, monetary damages and/or dismissal/termination from the School District. Some violations may constitute criminal offenses as defined by local, state and federal laws, and the School District may initiate or assist in the prosecution of any such violations to the full extent of the law.

2. Any suspected violation of this policy should be reported immediately to the Executive Director for Student Achievement and Instructional Technology, as well as to the Principal (if the suspected violator is a student), or the Superintendent of Schools (if the suspected violator is a faculty or staff member).

Additional Policies and Guidelines for Use of School District Computer Resources

Use of the School District's computer resources in the School District must comply with the following:

1. Cyberbullying, and sexting using sexually explicit, graphic, threatening or obscene language or images, or otherwise using language or images inconsistent with the values and general standards for community behavior of the School District are prohibited.
2. Anyone leaving such inappropriate messages on voice mail may face disciplinary action.
3. Anyone receiving a threatening message should record/save the message and report the incident to the Principal. The Executive Director for Student Achievement and Instructional Technology or his/her designee will attempt to trace the message and report the results to the Principal and the Superintendent of Schools.
4. Use of voice mailboxes for commercial purposes or advertising is not permitted.
5. Use of security codes is required in order to guarantee privacy for mailbox users.
6. Override permission codes are held by the Principals and the Library/Media Specialists in each school.

Wireless Policy and Guidelines

Cellular phones, pagers and walkie-talkies are provided to selected members of the School District by the Facilities Department. Wireless devices including, but not limited to, laptops, iPhones, iPod Touches, iPads and notebook computers are provided to staff members and/or students of the School District by the Executive Director for Student Achievement and Instructional Technology or his/her designee. The Facilities Department maintains the inventory for all these devices, auditing of wireless use by the staff, and efficient and effective resolution of billing and service-related issues. The use of wireless technology has been identified by the School District as useful in maintaining communications among the School District community and School District personnel in emergency situations or situations where immediate access to an employee is necessary. The use of such wireless technology is subject to the requirements of the School District's technology and telecommunications practices. By using wireless devices provided by the School District, the individual consents to the School District's exercise of its authority and rights as set out in this policy.

Cellular Phone Use

Purpose

All district-issued cellular phones shall be used for the purpose of supporting the School District's education and business objectives. This policy is intended to facilitate effective School District operations relating to cellular phone usage, encourage the responsible use of district-provided cellular phones, provide guidelines for appropriate cellular phone use, and help manage cellular phone usage costs.

Authorized Users

A list of those employees to whom cellular phones will be given for school business purposes shall be maintained by the Director of Facilities and reviewed annually by the Board of Education. This list shall also state with specificity, for each employee, the basis for the issuance of a School District cellular phone.

Acceptable Use Guidelines

1. Cellular phones shall be used only for necessary phone calls in furtherance of school business purposes. Charges or fees for personal cellular phone calls shall be reimbursed by the employee to the School District.
2. The School District shall monitor whether employee cellular phone use or expenses are unreasonable, excessive, personal, unauthorized, or unwarranted.
3. School District cellular phones shall not be used for the purpose of illegal transactions, harassment, obscene or offensive behavior, or other violations of School District policies or law.
4. Cellular phone service contract rights and equipment shall be the property of the School District, and any applicable determinations or changes as to them shall be made by the Business Office.
5. Employees shall have no expectation of privacy in the use of School District cellular phones. All cellular phone bills for district-issued phones are the property of the School District and will be used as appropriate to investigate the personal use of district-issued cellular phones.
6. School District cellular phones are valuable and should be handled with due care. If loss, theft, or damage to a School District cellular phone results from the known negligence of the employee to whom such phone is assigned, the employee will be required to reimburse the School District for the repair or purchase of replacement equipment.

7. Upon request, district-issued cellular phones shall be returned to the appropriate School District official.
8. The School District may discontinue cellular phone privileges at any time.

The Superintendent of Schools or his/her designee shall conduct regular cost-benefit analyses to determine whether the current cellular phone usage is advantageous to the School District, as well as whether cellular phone service plans should be changed in order to reduce costs and maximize the benefit to the School District.

Policy on Wireless Device/Radio Use

The School District insists that all employees act responsibly in their jobs so as not to endanger the lives of themselves or others. No telephone communication, business or personal, is so necessary or urgent that it cannot be postponed or interrupted until such time as the involved person can participate in the phone call without compromising safety. Safe driving is always the first responsibility. The School District actively discourages the use of hand-held cellular phones, and other wireless communication devices, while driving cars, trucks and golf carts both on and off campus, during School District work time or on School District business.

Further, employees should not dial, text, email or otherwise violate the law related to the use of electronic devices while driving on School District business. If an employee must engage in any of the above activities, he or she must pull over to a safe location off the roadway and out of traffic, stop and park the vehicle before doing so. Stopping in a roadway breakdown lane is by its very nature dangerous and therefore is not considered a safe location by the School District.

The School District acknowledges that members of the school administration, members of the facilities department and computer services and athletic trainers often use two way radios and radio-telephones in the School District in the performance of their daily duties. In addition, the use of wireless devices by building administration and security guards are both prevalent and necessary. These employees are reminded to use these devices in such a manner so as not to compromise safety.

The failure to comply with this policy may result in the loss of privileges/access to the School District's computer resources and possible disciplinary action consistent with law or the applicable collective bargaining agreement.

The Superintendent of Schools, working in conjunction with the designated Purchasing Agent for the School District, the computer network coordinator and the instructional materials planning committee, will be responsible for the purchase and distribution of computer software and hardware throughout the schools in the School District. They shall prepare and submit for the Board of Education's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or School District needs.

Failure to comply with School District policy and regulations for use of the network may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

Cross-ref: 8630, Computer Resources and Data Management

Adoption Date: April 11, 2019

Revised: April 11, 2019
December 12, 2024