COMPUTER NETWORK AND INTERNET ACCEPTABLE USE FOR STUDENTS AND STAFF

The Board of Education of the Great Neck Public Schools is committed to the optimization of student learning and teaching, considers an instructional computer network to be a valuable tool for education and encourages the use of computers and computer-related technology in District classrooms, and believes that providing access to computers is an integral part of a contemporary education. The term “education” includes use of the system for classroom, professional or career development activities. Through software applications, online databases, bulletin boards and electronic mail, the network can significantly enhance educational experiences and provide statewide, national and global communications opportunities for staff and students. Within financial limitations, computers, computer networks and the internet will be made available to students, faculty and staff. The technology resources at the 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 District and should be used for those purposes. An individual’s use of the District’s computer resources must be in support of education and research and consistent with the educational objectives of the District.

When an individual accesses computers, computer systems and/or computer networks, including the Internet provided by the District (hereinafter the “District’s computer resources”), the individual assumes certain responsibilities and obligations. Access to the District’s computer resources is subject to Federal, New York State and local law, as well as Board of Education policy. Use of District’s computer resources is a privilege to be used responsibly, fairly and appropriately, and is not a right. The District reserves the authority to control access to the Internet for all users of its computer resources. The District may either allow or prohibit certain kinds of online activity, or access to specific websites. Inappropriate use can result in the cancellation of privileges and/or disciplinary action by District officials.

The integration of technology with the curriculum is an essential part of instruction. At the same time, there is an inherent responsibility on the part of users to conduct themselves in an appropriate and considerate manner when using this medium. The Internet contains a rich array of educational content as well as information that is illegal or inappropriate for children. Therefore, Internet resources are filtered for inappropriate content, students are educated about Internet safety and digital citizenship, and student use is monitored and supervised by staff. However, the security, accuracy and quality of information that is available through District’s computer resources cannot be guaranteed.

Prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Superintendent of Schools or designee. To protect personal safety from risks involved with using the Internet, Internet users should not give out personal information to others on website, chat rooms or other systems. The 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. Users should be aware that District system administrators maintain compliance by monitoring online activity.

Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the District's computer resources to download illegally distributed material. In order to avoid damage to the District's computer resources, users are cautioned not to open e-mail attachments or download any files from unknown sources. Anything questionable should be reported immediately to a building administrator and/or the Superintendent of Schools or designee.

Parent/Guardian Option: A parent/guardian may deny their child independent access to the Internet at any time by submitting a letter to the school. However, teacher-directed Internet activities are part of our curriculum, and not subject to parent/guardian authorization.

Protection of Personal Information: Network activities increasingly include the use of various online educational Web sites and services that may require students to set up individual user accounts. When this is needed, the minimum required personal information will be provided solely for the purpose of accessing such services in connection with approved classroom instruction. With increased concern about identity theft and the need to protect personally identifiable information, teachers will consult with their school's technology specialist, and if needed, the District Technology Director, to ensure that the terms of service of any new cloud-based educational service complies with District standards for privacy and security, and are consistent with the *Parents' Bill of Rights For Data Privacy and Security (Policy 8635-E)*. Unless a parent/guardian denies such access for their child, students will be permitted to set up such accounts, with the consent of their teachers, in accordance with the Children's Online Privacy Protection Act (COPPA).

Internet Filtering System: In compliance with the Children's Internet Protection Act, (CIPA) the District employs technology protection measures that are designed to block access to visual depictions of pornography, obscenity and other material deemed illegal, inappropriate or harmful to minors. Web site traffic passes through this filter on all Internet-enabled computers. The following procedure has been developed to customize the filter in a manner that is consistent with instructional needs and community standards:

1. Three separate filters will be provided for students and staff to meet their respective educational, instructional, and professional needs while maintaining compliance with the law and this policy:
   a. elementary/middle school students;
   b. high school students;
   c. staff
2. Technology protection measures will not be disabled for student use. Bypass accounts will be limited in scope and by location to adult-only computers. The need to use bypass accounts should be rare; therefore, they will be provided to a limited subset of users including central and building administrators, deans, and computer and library staff. Bypass accounts will be provided for the following reasons:
   a. to conduct bona fide research for professional use;
   b. to preview blocked Web sites to determine their appropriateness for instruction;
   c. to investigate an issue involving the behavior, health, or safety of a student;
   d. for other lawful reasons not otherwise prohibited by the law or this policy.

   Staff members may access a bypass account through any of the users identified above. Users should be mindful of the fact that our filtering system logs all Web site activity.
3. Users are encouraged to submit Web site addresses that they believe are incorrectly filtered to their school's computer specialist for review.
4. Valid requests will be forwarded to the Office of Instructional Technology for resolution.
5. If a request is denied, alternatives will be discussed with the requestor and, if necessary, school library/technology staff will be consulted.
6. Uncategorized sites will be allowed by default on the staff filter, but will be blocked by default on student filters until they are categorized through the usual process or submitted for review.

Personal Security Issues: The Great Neck Public Schools issues network accounts and online accounts to students and staff to facilitate instruction and learning. The District also issues e-mail accounts to secondary students and staff to facilitate communication and collaboration. Information created with these accounts and stored on District equipment is the property of the Great Neck Public Schools, and is subject to District review. Therefore, users should have no expectation of privacy, and should exercise professional discretion when creating, storing or transmitting any electronic information including that which is stored on hosted providers. Likewise, online communications between students and staff offer unique learning opportunities, but can have potentially negative consequences if misused or misinterpreted. Students and staff should always be aware that online communications can become part of the public domain, and should not be considered personal or private.

1. Users should not share their school accounts or attempt to ascertain the passwords of others.
2. For safety reasons, students should never transmit personal information such as names, addresses, telephone numbers, or photographs, or make appointments with people they have met online, without prior authorization from both a parent/guardian and a building administrator or designee.
3. Students should notify a staff member whenever they come across information that is dangerous, illegal, obscene, inappropriate or makes them feel uncomfortable.
4. Users must follow the Guidelines in *District Sponsored Internet Publishing (Policy 5221)* to determine whether, and under what circumstances, names, photos, videos, school work, or other student or staff content may be published on public Web sites, including social networking sites.

Responsible Use:

1. All users must act in ways that comply with all legal restrictions regarding the use of electronic data and do not invade the privacy of others.
2. All users must maintain the confidentiality of student information in compliance with Federal and New York State law. Disclosing and/or gossiping (including but not limited to via e-mail, voice mail, Internet instant messaging, chat rooms or on Web pages) about confidential or proprietary information related to the District is prohibited.
3. All users must refrain from acts that monopolize the District's 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 circumvent filtering, access, degrade or tamper with the performance of the District's computer resources or telephone system or deprive authorized users of access to or use of such resources are prohibited.
4. Users are responsible for both the content and possible effects of their messages on the District's computer resources. 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 District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying, cyberbullying or harassing material), and billable services.
5. Official email communications must be professional, ethical and meet the standards of other District publications bearing in mind that the writer is acting as a representative of the District and in furtherance of the District's educational mission.
6. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in District email unless used in the furtherance of the business of the District or as part of the curriculum of the District. The signature

portion of the user's email may not include external links that are unrelated to the District and/or content of the email.

7. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.
8. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used with or on the District's computer resources except as permitted by law and approved by the Superintendent of Schools or designee. All software license provisions must be strictly adhered to.
9. Since the installation of applications, other than District-owned and District-tested programs could damage the District's computer resources or interfere with others' use, software downloaded from the Internet or obtained elsewhere must be approved by the Superintendent of Schools or designee. Software may not be installed onto any District- owned or District-leased computer by an individual other than the Superintendent of Schools or designee.
10. Use of voice mailboxes for commercial purposes or advertising is not permitted. Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use. Use of security codes is required in order to guarantee privacy for mailbox user.

User Guidelines: The same behavioral expectations of individuals in school and the community apply to use of the District's computer resources.

1. All student users of the District's computer resources will have access according to the student's assigned rights, with appropriate authorization and parent consent in writing. Approved class work will have priority over other uses. No single user should monopolize a computer, unless specifically assigned for special needs.
2. All use of the District's computer resources must be in support of education and research or administration/management consistent with the goals of the District.
3. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to access their accounts. Users will be held responsible for any policy violations that are traced to their accounts. Under no conditions will a user provide the user's password to another person.
4. Users will not meet with strangers they have met online.
5. Users may be required to remove files if District's computer resources storage space becomes low.
6. Users who are provided a District email address will check their email on a regular basis and delete unwanted messages promptly.
7. Electronic files stored on the school computers may be reviewed by school personnel at any time.
8. Priority will be given to those individuals who are using the Internet for curriculum-driven and research-oriented purposes.

9. The rights of all students and staff to use the District's computer resources without disruption should be respected at all times.
10. District-owned equipment and software should be treated with care.
11. Incidental personal use of the Internet is prohibited on the District network during the school day for all users, but is permitted for staff from 3 PM to 8 AM provided that such use does not interfere with a professional assignment, compromise network security or is in conflict with the educational philosophy of the Great Neck Public Schools. It is also permissible for staff to use personal devices that access the Internet without going through the District network, except during instructional, preparation, professional, and supervisory times as contractually defined. Students will follow the guidelines listed in the District's *Policy 5695 Personal Electronic Communication Devices*.
12. All staff and secondary school students will be assigned District e-mail accounts for professional and educational use.
13. Elementary school students can request e-mail access through a staff account for education-related reasons with authorization and supervision from the staff member.
14. Upon request, a club or activity may be assigned a District e-mail account to be used solely for the purpose of club or activity business. This account may be accessed by student designees, recommended and supervised by the faculty advisor.
15. Users may not access synchronous online communications such as chat rooms or instant messaging unless it is for education-related reasons; students must have authorization from a staff member.
16. High school students and staff members may access and contribute to asynchronous online communications such as message boards, blogs, and Wikis as long as messages are posted in a thoughtful and respectful manner for educational and professional reasons.
17. Elementary school students may participate in classroom activities that utilize software applications only if a teacher initiates the assignment and proactively reviews the posted content.
18. Users may utilize education-specific or professional social networking sites but not sites that primarily facilitate personal relationships. However, high school students and staff may request access to individual pages on such sites for educational or professional reasons.
19. 19.*The District and individual schools may have an official social networking presence as approved by the Superintendent of Schools or designee. School sanctioned clubs, activities and/or teams may have an official social networking presence, in accordance with Policy 4527 District Sponsored Social Media, with the approval of the building principal who must notify the District Office of Information and provide the account name(s).*
20. Image search sites are allowed for students and staff through a safe search filter, and video streaming sites are allowed for staff and high school students through a safe mode, or by exception.

21. Users may not download or upload files unless it is for education-related reasons; elementary and middle school students must have authorization from a designated staff member.
22. The use of the District's computer resources to purchase items or services for professional use, without appropriate supporting documentation, is prohibited.
23. High school students and staff members may use personal devices to connect to the appropriate District Bring Your Own Device (BYOD) wireless network in designated locations. By doing so, users implicitly agree to the terms, conditions, responsibilities, and liabilities for such use contained in this and other District policies as well as applicable local, New York State and Federal laws.
24. Adult visitors invited to the Great Neck Public Schools to conduct business, take adult education courses, or participate in evening, technology-based school events may use District equipment with guest network privileges. Requests for exceptions to this rule will be considered by the District Technology Director on a case-by-case basis. If an exception is granted, a temporary password will be made available for access to the BYOD Guest wireless network.
25. No user may physically or wirelessly connect unauthorized equipment of any kind to the District's network. Any such equipment, if found, will be removed immediately by District staff for network security reasons, and reported to the District Technology Director and Building Principal.

Prohibited Activities: The following is a list of examples of prohibited activity concerning use of the District's computer resources. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the District's computer resources.

- Knowingly or recklessly posting false or defamatory information about a person or organization.
- Utilizing the District's computer resources to access, create, download, edit, view, store, send or print material that is illegal, offensive, threatening, 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. For students, a special exception to certain sensitive materials for projects may be made for literature if the purpose of such access is to conduct research and the access is approved by the teacher or building administrator. The District's determination as to whether the nature of the material is considered offensive or objectionable is final. The District will respond to complaints of harassing or discriminatory use of the District's computer resources in accordance with *Policy 0100 Equal Opportunity*, *Policy 0110 Sexual Harassment* and/or *Policy 0115 Bullying and Harassment.*
  Attempting to log on through another person's account or to access another person's files, except that the District's administrators have the right to log on through another person's account and access another person's files for network security reasons or other reasons within their discretion.

- Using the District’s computer resources for a purpose or effect that is deemed by the Superintendent of Schools or designee to be dangerous, objectionable, pornographic, distracting to education, or otherwise offensive in nature.
- Engaging in any illegal act, such as arranging for a drug sale, purchasing alcohol, engaging in criminal activity, threatening the safety of a person, etc.
- Unauthorized exploration of the Network Operating System or unauthorized changes to any installed software.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy District equipment or materials, data of another user of the District’s computer resources or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network. Unauthorized tampering or mechanical alteration, including software configurations is considered to be vandalism
- Using the District’s computer resources to send anonymous messages or files.
- Using the District’s computer resources to receive, transmit or make available to others a message that is inconsistent with the *District’s Code of Conduct (Policy 5300).*
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the District’s computer resources for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Using District’s computer resources for commercial purposes or financial gain or fraud.
- Using the District’s computer resources for political purposes, including political lobbying in support of or opposition to individual candidates or political parties.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Changing or exceeding resource quotas as set by the District without the permission of the appropriate District official or employee.
- Using the District’s computer resources while access privileges are suspended or revoked.
- Using the District’s computer resources in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Invading the privacy of others.
- Failing to comply with all legal restrictions regarding the use of electronic data

.

- Sending broadcast e-mail or broadcast voice mail.
- Using the District's computer resources for private or commercial business, advertising or religious purposes.
- Student recording of classroom instruction without the express permission of the teacher.
- Attempting to gain unauthorized access to the District system or to any other computer system through the District System, or go beyond authorized access. This includes attempting to access another person's files.
- Deliberately attempting to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.
- Engaging in illegal acts, such as computer fraud, threatening the safety of self or others, hacking, or engaging in any activity that violates local, New York State, or Federal laws.
- Damaging District technology in any way.
- Installing software to District technology, including any downloads, games, hacking tools, music sharing or video sharing applications or others or attempting to run such software from a personal device such as a thumb/flash drive or any other media/device.
- Transmitting inappropriate pictures of themselves or others.
- Attempting to find security problems, as this effort may be construed as an attempt to gain illegal access to the network.
- Attempting to gain unauthorized access to files stored on computers or network servers.
- Using the District's computer resources to post materials or establish email accounts unless required and authorized as part of a curriculum project.

Terms and Conditions for Personal Devices: BYOD wireless networks for high school students and staff are designed to provide wireless access to the Internet and may not have access to other networked District resources. In addition to the other guidelines in this policy, the following terms are pre-conditions for the use of personal devices on our BYOD wireless networks:

1. Personal devices must contain the most recent operating system, security updates, Web browser, and virus/malware scanning software (where applicable).
2. Technical information about personal devices may be logged by the District when making this connection.
3. High school students and staff agree to submit their personal devices to GNPS Technical Support or school staff upon request for ongoing compliance with these guidelines.
4. GNPS Technical Support is not available to troubleshoot or support personal device issues.
5. The District is not responsible or liable if personal devices are accessed, modified, infected, broken, vandalized, stolen, lose data, become inoperable,

injure the owner or another individual, or damage the property of the school or others while on District property.

Ethical and Legal Considerations: Use of the District's computer resources must conform to District policies and local, New York State and Federal laws. The following are prohibited:

- Use of the District to access, store, distribute or promote illegal activities, obscenity or any other material deemed inappropriate or harmful to minors.
- Use of the District to install, use, store, duplicate or distribute personal software or copyrighted materials without the permission of the appropriate District official or employee or license to do so, including software, files, videos, photographs, graphics, text, music, or speech.
- Use of the District computer resources to transmit computer viruses or other malware.
- Use of the District to plagiarize, in part or whole, the intellectual property of others, including the work of fellow students or any published content whether in print or electronic format.

District Limitation of Liability: The District does not warrant in any manner, expressed or implied, that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the user's own negligence or the errors or omissions of any user.

Similarly, the District will not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

In accordance with *Policy 8332 District-Issued Portable Electronic Devices*, users are responsible for any financial costs, liabilities, or damages incurred by the District as a result of improper use of District computer resources, including, but not limited to, equipment (including repairs), replacement of and/or insurance for Chromebooks/iPads or other District issued technological devices, legal fees, and other costs.

Consequences of Violations: The consequences for violating this policy will be consistent with other District policies and may include the following:

1. Notification of school authorities.
2. Notification of parent/guardian.
3. Suspension of access to the District's computer resources and the Internet.
4. School consequences consistent with *Policy 5300 Code of Conduct*.
5. Financial restitution.
6. Legal action.

Staff Responsibilities: In order to comply with the provisions of this policy and CIPA, building principals will inform staff members to:

1. Inform all students about the guidelines contained in this policy, educate all students with regard to Internet safety and digital citizenship, and supervise and monitor the online activities of all students.
2. Take reasonable measures to prevent students whose parent/guardian has denied permission from engaging in independent Internet activities.
3. Take appropriate disciplinary actions when students violate this policy.
4. Report serious policy violations to an administrator.
5. Report illegal, obscene, or inappropriate information to the Office of Instructional Technology.
6. Never facilitate the collection of private information about students by any Web site outside of the Great Neck Public School domain, consult with the school's technology specialist, and if necessary, the District Technology Director, to ensure cloud-based services comply with District standards for privacy and security of personal information, and ensure that only the minimum information has been provided to conduct a sanctioned online educational activity.
7. Contact an administrator when inappropriate student use of the Internet outside of school comes to their attention so that the matter can be investigated, parents/guardians may be notified, and appropriate action may be taken to minimize disruption to the educational environment and ensure the safety and well-being of children.

All of the above notwithstanding, parents/guardians are ultimately responsible for the appropriate behavior of their children when using personal or District-issued technology outside of school and should address any misuse or misbehavior.

Great Neck Public Schools
Adopted: 4/28/98
Amended: 6/17/02; 1/09/06; 3/31/08; 6/21/10; 12/9/13; 7/7/15; 9/16/20; 2/16/22; 3/9/22