COMPUTER NETWORK AND INTERNET ACCEPTABLE USE FOR STUDENTS AND STAFF

Philosophy: It is the philosophy of the Great Neck Public Schools that 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 our network cannot be guaranteed.

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 *Policy 5550-E Parents' Bill of Rights For Data Privacy and Security*. 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.

Internet Filtering System: In compliance with the Children's Internet Protection Act, 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 high school 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 his/her 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 *Policy 5221 District Sponsored Internet Publishing* 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.

User Guidelines: Use of our network is a privilege to be used responsibly, fairly and appropriately. The same behavioral expectations of individuals in school and the community apply to online behavior. Users should be aware that the District maintains compliance by monitoring online activity.

1. Priority will be given to those individuals who are using the Internet for curriculum-driven and research-oriented purposes.

2. The rights of all students and staff to use our network without disruption should be respected at all times.

3. District-owned equipment and software should be treated with care.

4. 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.*

5. High school students and staff members will be assigned District e-mail accounts for professional and educational use.

6. Elementary and middle school students can request e-mail access through a staff account for education-related reasons with authorization and supervision from the staff member.

7. 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.

8. 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.

9. High schools 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.

10. Elementary and middle school students may participate in classroom activities that utilize e-mail and Web 2.0 applications only if a teacher initiates the assignment and proactively reviews the posted content.

11. 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.

12. The District as an organization, and the individual schools as suborganizations, may have, to the extent possible, an official read-only social networking presence using Facebook® with a designated computer to be used for this purpose. High school students may participate in maintaining a school's official social networking presence using Facebook® with supervision by a designated staff member. Clubs, activities, teams, and other groups may contribute to the suborganization presence.

13. Image search sites are allowed for students and staff through a safe search filter, and video streaming sites are allowed for high school students and staff through a safe mode, or by exception.

14. 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.

15. The use of the District network to purchase items or services for professional use, without appropriate supporting documentation, is prohibited. Personal purchases by staff are permitted 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.

16. Users may not attempt to gain unauthorized access to other user accounts, hack into computer systems, breach security passwords or circumvent our filter.

17. 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, state and federal laws.

18. 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.

19. No users may physically or wirelessly connect unauthorized equipment of any kind to our 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.

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 our computer network must conform to District policies and local, state and federal laws. The following are prohibited:

1. Use of our network to access, store, distribute or promote illegal activities, obscenity or any other material deemed inappropriate or harmful to minors.

2. Use of our network to install, use, store, duplicate or distribute personal software or copyrighted materials without the license to do so, including software, files, videos, photographs, graphics, text, music, or speech.

3. Use of our network to transmit computer viruses or other malware.

4. Use of our network 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.

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 computer network and the Internet.

4. School consequences consistent with the *Policy 5300 Code of Conduct*.

5. Financial restitution.

6. Legal action.

Staff Responsibilities: In order to comply with the provisions of this policy and the Children's Internet Protection Act, 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 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 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