

Created: 01/08/2008 **Revised:** 07/10/2008

PURPOSE: These procedures define the responsibilities of Newport News Public Schools employees, [Non-Employees](#), volunteers, and students using the computers, telecommunications, network and Internet resources provided by the school division. Every [authorized user](#) is required to read and acknowledge these procedures either by signing the appropriate use agreement form or the [online acknowledgement form](#). Student forms will be filed in their school offices. All other user forms will be on file in the Human Resources office.

SCOPE: All Newport News Public School (NNPS) employees, Non-Employees, Volunteers and Student Use.

STATEMENT OF

PROCEDURE: Use of the [NNPS Computer System](#) by persons other than students should consist of activities necessary to support the purpose, goals and mission of NNPS. The following, although not inclusive, define specific acceptable and unacceptable uses of the NNPS Computer System.

1. Privacy:

Communications over the division's network shall be considered public information and handled as such. The NNPS Computer System authorized users must not have and shall have no expectation of privacy in their use of the Computer System. All information created, sent received, accessed, or stored in the NNPS Computer System is subject to inspection and monitoring at any time and may occur without notice to users. Technology Services may periodically review directories or messages to determine compliance with policy IJND for acceptable use. If unacceptable content or use is found, access privileges may be removed and the offender counseled at an appropriate level as outline in section 12, Violations and Penalties, of this procedure.

2. Security:

Access is restricted to the NNPS Computer System and authorized users. Authorized users are responsible for their individual account information and should take all precautions to prevent others from accessing their account. Authorized users are prohibited from knowingly disclosing or modifying any assigned or entrusted access control to their account (such as: log-in identifiers, passwords, terminal identifiers, user identifiers, digital certificates, Internet Protocol (IP) addresses, etc.) for any purpose other than those required to perform authorized NNPS functions. Authorized users may only access, modify or destroy files, data and resources for which they are authorized and that lie within the scope of their responsibilities, and only in accordance with Virginia Electronic Records Guidelines. Malicious destruction or modification of data or resources is prohibited.

All NNPS employees should immediately notify an administrator, principal or teacher if they have identified a possible security breach.

Authorized users will not attempt to go beyond their authorized access to the NNPS Computer System. This includes attempting to log into the NNPS Computer System through another authorized user account or accessing or attempting to access another authorized user's file without authorization. Unauthorized access is illegal, even if only for the purpose of browsing.

Authorized users will not deliberately attempt to disrupt the NNPS Computer System performance or destroy data by spreading computer viruses or by any other means.

At no time is a connection authorized to the [NNPS Local Area Network](#) via a non NNPS Computer System device.

3. Facsimile (Fax):

Fax machines are to be used by authorized users. These machines are not to be used for sending or receiving personal correspondence. Any sender of personal correspondence is to be notified by the receiver to cease transmitting personal correspondence. Any review, dissemination or use of the fax transmission by a person other than the addressee is prohibited. Students are not authorized to use NNPS fax machines unless permission has been granted by an NNPS employee.

4. Telephone Service:

NNPS telephone service, to include landlines and cellular telephones, is to be used primarily for making calls regarding students and other school business. The use of school division phones for personal business should be kept to a minimum.

Occasionally it may be necessary for employees to place a long distance call using the school phone. If these calls are for school business callers must complete, at the time of the call, Exhibit E: Long Distance Call Log to record each long distance business call.

Personal long distance calls at school are discouraged; however, should they become necessary and with approval from the facility administrator, arrangements will be made to pay for the cost of the long distance call. Callers will complete, at the time of the call, Exhibit E: Long Distance Call Log to record each personal long distance call.

On the last working day of each month the facility administrator will submit the Exhibit E: Long Distance Call Logs to Technology Services, Communications Department. The call logs will be reviewed and compared against the corresponding monthly long distance phone bill. The accounting department will be notified of all personal long distance phone calls to coordinate reimbursement to the division.

5. Copyright:

Division policies on copyright will govern the use of materials accessed through the NNPS Computer System. Because the extent of copyright protection of some information found on the Internet is unclear, users will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an [infringement](#).

Teachers will instruct students to respect copyrights and to request permission when appropriate.

Users must not knowingly load onto the NNPS Computer System or use commercial software in violation of its copyright and/or licensing agreement and will not perform downloads or installs without the authorization of the Technology Department.

6. NNPS Computer System Software:

Only division approved and provided software shall be loaded on the NNPS Computer System. No software such as applications, games, freeware, demonstration software, and shareware shall be downloaded or installed on device in the NNPS Computer System without written approval from Technology Support Services Supervisor.

7. Academic Freedom, Selection of Material, Student Rights to Free Speech:

Federal and State Laws on academic freedom and free speech will govern the use of the Internet. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to course objectives. Teachers will preview materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site.

8. NNPS Websites:

NNPS has established a Web site and Web pages that present information about the school division. The Superintendent will designate an administrator to be responsible for maintaining the division Web Site. The principals or their designee(s) are responsible for overseeing the development and content of their school's web site and for ensuring that published content is relevant to the department/school and complies with the AUP Policy.

School Board policy GBAA, Discrimination and Harassment applies fully to the NNPS published Internet sites. Abusive, vulgar, harassing, threatening or otherwise inappropriate content will not be published on School Board owned Internet sites.

NNPS web sites will not post photographs of our student population without permission from a parent or legal guardian. Student forms will be filed in their school offices. All other user forms will be on file in the Human Resources office.

NNPS websites will not contain direct links to pages that violate the AUP policy.

9. Electronic Mail (e-mail):

The NNPS e-mail system provides authorized users the capability of sending and receiving electronic communications between all schools and the central office in addition to electronic communications outside the school division. Use of the e-mail system should pertain to school related business only.

Authorized users will check their e-mail frequently and delete unwanted messages promptly. E-mails required to be filed for extended periods of time should be archived to CD or electronically stored outside the e-mail system.

As normal policy, students are not granted access to e-mail however, for special projects and programs, students will be granted access to the e-mail system for the duration of the program or project. It is the program or project administrator's responsibility to ensure the e-mail system is not abused or used in a matter other than described in the AUP for such programs and projects.

E-mails are written records and may be subject to inspection and monitoring without notice to the user. Users must not have and shall have no expectation of privacy in e-mail. In addition, disclosure may occur pursuant to the Virginia Freedom of Information Act (FIOA), Code of Virginia, §2.2-3700 et seq., legal process and civil discovery, and division reviews and maintenance. The following are examples of inappropriate uses:

- Authorized users will not engage in [spamming](#).
- Authorized users will not use the e-mail systems for personal gain, commercial purposes, or political lobbying.
- It is prohibited to use e-mail for the propagation of viruses, computer worms, Trojan Horses, and other malicious software acts.
- Authorized users will not engage in [phishing](#).

- Authorized users will not transmit threatening, abusive, vulgar, obscene, or harassing e-mails.
- It is prohibited to attempt to subscribe an authorized user to any electronic mailing lists.
- With the exception of the NNPS [web based e-mail](#) system it is prohibited to access any web based e-mail system from any NNPS Computer System.

10. Text Messaging:

[Text messaging](#) may be provided to those authorized users requiring cellular service as part of the job requirements for NNPS. Text messaging is not provided by default on a NNPS provided cellular device. Use of text-messaging should pertain to school related business only.

Authorized users must request that text messaging service be turned on for their approved cellular device and provide justification for its use in the performance of the users' duties.

Text messages are written records and may be subject to inspection and monitoring without notice to the user. Users must not have and shall have no expectation of privacy in text messaging. In addition, disclosure may occur pursuant to the Virginia Freedom of Information Act (FIOA), Code of Virginia, §2.2-3700 et seq., legal process and civil discovery, and division reviews and maintenance.

11. Internet Safety and Ethics

The NNPS Computer System will not be used to send, receive, view or download illegal/undesirable content/materials or to conduct illegal activities (e.g. arranging for the sale/purchase of drugs, engaging in criminal gang activity, pornography or threatening the safety of another individual). It is prohibited to use electronic communication services for fraudulent, threatening, obscene, rude, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages. In addition, the NNPS Computer System will not be used for commercial purposes, personal gain, or political lobbying.

Restrictions against inappropriate language apply to public messages, private messages and material posted on Web pages. Authorized users will conduct themselves in a manner that is appropriate and proper as representatives of the school division.

Authorized users will subscribe only to discussion group mail lists that are school division sponsored/authorized, affiliated and/or relevant to school business. Authorized users will not access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature only if the purpose of such access is to conduct research and access is approved both by the teacher and the parents or legal guardian.

The Children's Internet Protection Act (CIPA) requires schools and libraries receiving E-Rate discounts for Internet access and internal connections to comply with the CIPA. NNPS has implemented an Internet Filter to block access to text and [visual](#) depictions deemed "obscene", "child pornography," or "harmful to minors."

Internet filters are not fail-proof and therefore may not block all undesirable Web pages. Therefore, authorized users will only be allowed access to the Internet to pursue education-related activities. Teachers must keep up-to-date on Internet safety issues and provide accurate, timely information to students. Teachers will establish and post rules for safe Internet use near computers in classrooms, libraries and labs and remind students regularly that the rules are intended to ensure safety. Teachers should immediately notify an administrator, principal or Technology Services if they have identified a possible CIPA issue.

Authorized users will not post personal contact information about themselves or other people. Personal contact information includes school or work addresses, telephone numbers, etc. Students will not agree to meet with someone they have met online without the approval of their parents or legal guardians.

12. Violations and Penalties

Authorized users will be given notice of violations and given an opportunity to provide explanation for determination regarding continuing access to the NNPS Computer System. Privileges may be suspended immediately. For employees, disciplinary action may be taken. Violations of the law will be reported to law enforcement officials. NNPS will cooperate fully with local, state, and federal officials in any investigation related to illegal activities conducted using the NNPS Computer System.

Disciplinary action related to student access to electronic resources may be determined at the building and/or classroom level in accordance with existing policies and procedures as stated in School Board Policy JI, Student Rights and Responsibilities, and/or other School Board Policies and Procedures governing student discipline. Disciplinary actions should be tailored to assist the student in gaining the self-discipline to behave appropriately on an electronic network.

13. Definitions:

- [Non-employees:](#) Contractors and support personnel who directly support the goals and mission of NNPS.
- [NNPS Computer System:](#) A computer system that is owned, purchased, and/or supported by NNPS, and includes all technology resources and access to telecommunications networks (e.g. internet, local and wide area networks, hardware, software and communications services) division-wide and remotely.
- [Authorized User:](#) A NNPS Computer System user whose access privileges have not been suspended or revoked.
- [NNPS Local Area Network:](#) The computer network using the private Internet Protocol (IP) address scheme (not directly accessible from the Internet) defined by NNPS Technology Services and accessed by wired or wireless connections.
- [Infringement:](#) When an individual inappropriately reproduces a work that is protected by a copyright.
- [Spamming:](#) An e-mail user sending annoying, non school business, or unnecessary message(s) to an individual or a large number of people on a specific e-mail list or site.
- [Phishing:](#) The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to persuade the user to surrender private information that will be used for identity theft.
- [Web based e-mail:](#) A web based system that performs the functions of a mail client allowing access to e-mail through the Internet.
- [Text messaging:](#) Text messaging is the common term for the sending of "short" (160 characters or fewer, including spaces) text messages from mobile phones using the Short Message Service (SMS).
- The [Online acknowledgement form](#) is an electronic form for NNPS employees to electronically acknowledging the AUP. The url is: <https://secure.nn.k12.va.us/aup/>

14. Disclaimer

The School Board will not be responsible for any information that may be lost, damaged or unavailable when using the NNPS Computer System or for any information retrieved from the Internet.

The School Board is not responsible for any unauthorized charge or fee resulting from the use of the NNPS Computer System.

In the event filtering software, used to screen Internet sites for offensive material, is unsuccessful and authorized users gain access to inappropriate and /or harmful material, the School Board will not be liable.

Every effort will be made to avoid the violation of privacy of individuals or groups; however, NNPS Computer System authorized users have no right of privacy and should have no expectation of privacy in materials sent, received, or stored in School Board owned equipment within the NNPS Computer System.

**OTHER
POLICIES:**

- School Board Policy IJND: Acceptable Use Policy
- School Board Policy GBAA: Discrimination and Harassment

AUTHORITY

REFERENCE:

- Code of Virginia, §22.1-70.2
 - *(Acceptable Internet use policies for public and private schools)*
- Children's Internet Protection Act
 - *(Federal Communications Commission (Consumer & Governmental Affairs Bureau))*
- The Library of Virginia
- Virginia Department of Education

OTHER

REFERENCE:

- Technology Services Memorandum: Division Owned Cell Phones
- Technology Procedure: Technology Standards and Procedures
- School Board Exhibit IJND-E: Employee, Non-Employee, and Volunteer Acceptance Form
- School Board Exhibit IJND-E: Student Acceptance Form
- School Board Exhibit IJND-E: Long Distant Call Log