# Northland Preparatory Academy

**Title: STUDENT ACCEPTABLE USE OF THE NPA NETWORK**
**Submitted to Governing Board:** 26 September, 2005

This policy sets forth the standards governing Northland Preparatory Academy ("NPA") students' use of the NPA network as well as the Student BYOD network. This policy also sets forth the rules under which student authorized users may continue their access to and use of these resources. This policy promotes the ethical, legal, and school-related use of the NPA Network and ensures NPA compliance with the Children's Internet Protection Act. Personal electronic devices will be governed under this policy when such devices are attached to the NPA network. Students using their own devices may not access inappropriate material on their own network at school or any school event. Authorized student use of information resources must be consistent with the educational purposes for which these resources have been provided. Use of the NPA Network is a privilege that is provided to help student authorized users complete and deliver educational obligations. The NPA Network provides student authorized users with the means for communicating effectively with schools, teachers, administrators, the public, other government entities, and educational experts. These resources should be used in a manner that both enhances students' educational experiences and complies with this policy and regulations established from time to time by the Northland Preparatory Governing Board ("Board"). NPA students, through their use of the NPA Network, will gain skills and expertise that prepare them for an increasingly technology-oriented society.

**I. DEFINITIONS**

**A. Northland Preparatory Academy's Network ("NPA Network")** is the system of computers, terminals, servers, databases, routers, hubs, switches and distance learning equipment connected to the NPA Network.

**B. Electronic Mail (e-mail)** consists of all electronically transmitted information including any combinations of text, graphics, audio, pictorial, or other information created on or received by a computer application system and includes the transmission data, message text, and all attachments.

**Other Electronic Devices** include, but are not limited to, cellphones, tablets, laptops, and electronic readers that may or may not be physically connected to the network infrastructure.

**C. Password** is a secret word or series of letters and numbers that must be used to gain access to an online service or the Internet or to modify certain software (such as parental controls).

**D. Student Authorized Users** are any students enrolled in any classes offered by NPA in a traditional classroom or virtual classroom setting.

**II. GENERAL PROVISIONS**

**A. AUTHORIZED USERS**

All student authorized users shall adhere to the provisions of this policy as a condition for continued use of the NPA Network. It is a general policy of NPA to promote the use of computers in a manner that is responsible, legal and appropriate. This policy is enacted anytime there is a connection to NPA's hardwired or wireless network and other personal electronic devices.

**B. DISCLAIMER**

Pursuant to the Children's Internet Protection Act, NPA uses filtering software to screen Internet sites for offensive material. The Internet is a collection of worldwide networks and organizations that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Tasteless; and Illegal/Questionable. In general it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Authorized users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and children and staff gain access to inappropriate and/or harmful material, the Board will not be liable. To minimize these risks, authorized use of the NPA Network is governed by this policy.

## III. TERMS AND CONDITIONS FOR AUTHORIZED USE OF THE NPA NETWORK

### A. ACCEPTABLE USES

NPA students may use the various resources provided by the NPA Network to pursue educationally-related activities. Teachers and other staff should help guide students in their use of the NPA network so that students will learn how Internet resources such as, instant messaging and chat rooms can provide valuable educational information from classrooms, schools, and other national and international sources. In addition to using the NPA Network for educational pursuits, users will be expected to follow generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in your messages to others.
2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
3. Keep personal information, including the logins, passwords, addresses, and telephone numbers of students or colleagues confidential.
4. Use these resources so as not to disrupt service to other student authorized users.
5. Do not upload, post, e-mail, transmit, or otherwise make available any content that is unlawful, dangerous or may cause a security risk.

**B. UNACCEPTABLE USES**

Improper use of the NPA network is prohibited. Actions that constitute unacceptable uses of the NPA network and are not specifically addressed elsewhere in this policy include, but are not limited to:

6. Use of the NPA network for, or in support of, any illegal purposes.
7. Use of the NPA network for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If a student authorized user inadvertently accesses such information, he or she should immediately disclose the inadvertent access to a teacher or to the school principal. This will protect the user against allegations of intentionally violating this policy.
8. Use of the NPA network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or "stalk" another individual.
9. Non-educational uses of the NPA network including, but not limited to games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities or political lobbying.
10. Using Internet tools such as social media, chat rooms, and instant messaging for personal rather than educational purposes.
11. Using profanity, obscenity or language that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities.
12. Plagiarizing any information gained on or through use of the NPA network or any other network access provider.
13. Using copyrighted materials, including commercial software, without permission of the copyright holder, and in violation of state, federal or international copyright laws. (If students are unsure whether or not they are using materials in violation of copyright provisions, they should ask their teachers or a school technology coordinator for assistance.
14. Violating of any provision of Family Educational Rights and Privacy Act (FERPA), which governs students' rights to privacy and the confidential maintenance of certain information including, but not limited to, a student's grades and test scores is prohibited.
15. Using the NPA Network for financial gain or for the transaction of any business or commercial activities.

**C. SECURITY**

All authorized users are to report promptly any breaches of security violations of acceptable use and the transmission of web addresses or e-mail information containing inappropriate material to their teacher or the school principal. Failure to report any incident promptly may subject the authorized user to disciplinary action. In order to maintain the security of the NPA System, students are prohibited from engaging in the following actions:

- Intentionally disrupting the use of the NPA network for other users including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, or engaging in "hacking" of any kind, which is an illegal or unlawful entry into an electronic system to gain secret

unauthorized information.

- Unintentionally spreading computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a computer system without authorization or for damaging or altering without authorization the software components of a computer or computer system.
- Disclosing the contents or existence of NPA computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients. Authorized users must not share logins or password(s) and unauthorized information regarding other users' passwords or security systems.
- Downloading unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet.

**IV. MONITORING**

The NPA Network is routinely monitored to maintain the efficiency of the system. Authorized users should be aware that use of the NPA Network, including their use of e-mail, is subject to reasonable and appropriate monitoring. Any activities related to or in support of violations of this policy may be reported and will subject the user to sanctions.

**V. ASSUMPTION OF RISK**

NPA will make a good faith effort to keep the NPA Network system and its available information accurate. However, student authorized users acknowledge that there is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available. Use of the NPA Network is at the risk of the student authorized user.

**VI. INDEMNIFICATION**

The student authorized user indemnifies and holds NPA harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the NPA network that cause direct or indirect damage to the user, NPA, or third parties.

**VII.SANCTIONS**

Failure to abide by this policy may subject the student authorized user to corrective action ranging from suspension of some or all access privileges up to and including expulsion. A violator must understand that if his or her privileges to use the NPA Network are revoked by a school faculty member that he or she has the right to appeal the revocation within thirty (30) days, in writing, to the principal of the school. The school principal's decision shall be FINAL. A violator must understand that if he or she is removed from the NPA network, there shall be no obligation to provide a subsequent opportunity to access the NPA network.