TECHNOLOGY ACCEPTABLE USE POLICY FOR STAFF AND STUDENTS

The School Committee recognizes that knowledgeable use of computer technologies and the Internet are necessary skills in every aspect of modern day society. By providing Intranet and Internet access to staff and students, we promote educational excellence in the schools and facilitate resource sharing and communication, so that staff and students may access these systems to pursue intellectual activities, seek vast, diverse, and unique resources, access libraries, and engage in learning activities within a global community.

The intent of this policy is to frame the use of these networks only for purposes consistent with our educational mission. All school computers are to be used in a responsible, efficient, ethical, and legal manner. The codes of conduct of the schools apply to Internet activities, and this Acceptable Use Policy should therefore be considered an extension of the staff and students' codes of conduct and district policies. In order to provide a proper message to the community, staff-posted content on the Internet includes, but is not limited to, material that supports the curriculum and instruction, general information that supports student safety, growth, and learning, or public information of interest to others. We expect that such content shall be responsibly developed and professionally delivered, and correct for the target audience. Moreover, in order to maintain the safety of the Northampton Public School district's students, use of student work, pictures of students, or any other information that would allow for the identification of any student is forbidden without the express written permission of the parent or guardian of any student concerned. Student work may be published only as it relates to a class project, course, or other school-related activity.

Individuals who log on to the Internet at school are responsible for all activities while using their account. Therefore, users should not share passwords and should change their passwords frequently. Users should also exercise caution when revealing personal information. To ensure personal safety and the safety of others, users should not publish their home address, phone number, or any other confidential information over the Internet. If students experience any concerns over communications they have received from others over the Internet, they should seek assistance from staff or parents immediately.

In accordance with the Children's Internet Protection Act (CIPA), passed by the U.S. Legislature in January 2001 (Public Law 106-554), our schools shall employ filtering software to block access to inappropriate content on all computers with Internet access. Users will be restricted from accessing visual depictions of subject matter that is obscene, pornographic, or harmful to minors. Users should furthermore be aware that filtering software will not block ALL inappropriate websites (e.g. new sites that have not yet been added to the filter lists). Members of the school community shall report all inappropriate sites not blocked by the filters to a technology administrator for appropriate action. Filtering software may be disabled for users 18 and over by a technology administrator for legitimate research purposes.

Our schools have software and systems in place that monitor and record all Internet usage. The District will intermittently monitor Internet network traffic and other usage of electronic resources, for instance, by tracking destination URLs of individual users. Users should have no expectation of privacy when browsing the web, sending or receiving email, or using other electronic school resources. The District does provide email accounts for the purpose of school related communication.

Our Users

Recognizing that collaboration is essential to education, The District may provide our users (staff/students/volunteers) with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Access to district network systems is a privilege, not a right. Unethical or illegal use of school computers, or use for other than legitimate educational use, will be cause for disciplinary action, including, but not limited to, revocation of network access privileges, suspension and/or referral to the police or other appropriate authorities.

Examples of such inappropriate uses include unauthorized access into school accounts or private files, destruction of others' files, harassment of students or staff, introduction of computer viruses, unauthorized downloading of programs or content, commercial use of school networks, violation of copyright laws, use of inappropriate language, and transmissions of or searches for obscene material. Should vandalism occur, the individual responsible may be held accountable for the cost of damages, repairs, or necessary replacement. Additionally, the rules and regulations set forth in the Student Handbook may also be applied.

Noncompliance with applicable regulations and procedures may result in suspension or termination of user privileges and other disciplinary actions consistent with the policies of the Northampton Public Schools. Violations of law may result in criminal prosecution as well as disciplinary action by the Northampton Public Schools.

Additionally, the Northampton Public Schools shall not be liable for users' inappropriate use of electronic resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The Northampton Public Schools shall not be responsible for ensuring the accuracy or usability of any information found on external networks.

Adoption date:	November 2001
Amended:	May 12, 2005 February 14, 2013