

ACCEPTABLE USE OF COMPUTING SYSTEMS BY STUDENTS

Each day in Newport News Public Schools the focus is on one mission: ensuring that all students graduate college, career and citizen-ready! The division provides a wide range of computing systems to students to promote educational excellence in schools by facilitating research, resource sharing, communications, creativity, and collaboration. The use of these computing systems shall be consistent with School Board Policy IJND – Technology Acceptable Use.

For the purposes of this document, “computing systems” refers to all electronic tools that have relevant uses for education, including but not limited to computing hardware, software, peripherals, networks, network resources, electronic files, and Internet access. All NNPS computing systems are the property of the division and are intended for conducting official school and/or division business only.

Acceptable use of NNPS computing systems by students is defined as use for educational purposes and in ways that adhere to the policies and procedures present in the division as well as to applicable state and federal laws.

Unacceptable use of NNPS computing systems includes but is not limited to harassment, solicitation, threatening, bullying, communicating obscenities, engaging in commerce, gambling, and accessing prohibited materials. Further comments about acceptable and unacceptable use are outlined in the bullet points below:

Digital Citizenship and Internet Safety

- Students will be educated in safe and productive practices for using technology by their teacher or another appropriate employee. Students should exercise good judgment at all times when using technology resources.
- The material you accessed through the computing systems should be for class assignments or for personal research on subjects similar to what you might study in a class or in the school library. Use for entertainment purposes is not allowed.

Cyberbullying

- Students shall not harass or bully others online. Cyberbullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures, or images, or website postings.

Communication and Content Privacy

- Students should not have an expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received and/or stored on NNPS computing systems.
- Authorized employees may review any student's communications or any electronic content created by the student using NNPS computing systems for the purpose of monitoring adherence to acceptable use and do not need the student's permission to do so.
- The district will cooperate fully with local, state, and federal officials in any investigation related to any unlawful activities conducted through the district's network system.

Security

- Students are responsible for their own individual accounts and files. User IDs and passwords are provided for each user's personal use only. Passwords should not be shared with anyone. Students must not use another person's password. If you suspect that someone has discovered your password, you must have it changed immediately.
- Students should not attempt to gain unauthorized access to the district's computing systems or any other computer system through the district's network system or go beyond your authorized access. This includes attempting to log in through another person's account or to access another person's files.

Copyright

- Any copyrighted materials accessed through NNPS computing systems remain copyrighted and may be subject to the Fair Use provisions of copyright law as they relate to education. Information concerning Fair Use can be found in each school library.

ACCEPTABLE USE OF COMPUTING SYSTEMS BY STUDENTS

Software

- Only division approved software shall be loaded on NNPS computing systems. No software shall be downloaded from the Internet and/or installed on any NNPS computing system unless expressly arranged by Technology.
- Students shall comply with all hardware and software licensing agreements. Students may request software if it is used for educational purposes.

Undesirable Materials

- The division has installed filtering software to protect against access to inappropriate material as required by the Children's Internet Protection Act ("CIPA"). While students are accessing NNPS computing systems, the division will take all reasonable precautions to restrict students' access to undesirable materials. However, students must also accept responsibility for avoiding access to such materials when possible.
- Students who gain access to undesirable materials via NNPS computing systems shall alert their teacher or another appropriate employee for reporting to the building administrator and/or Technology.
- Students should not seek to bypass filtering software by using proxies or other technologies.

Social Networking Technologies

- Nothing in the aspect of, access to, or operation of social networking technologies (whether in the form of software, websites, hardware, or other technologies) shall exempt students from the same procedures and responsibilities established elsewhere in this document.
- Additionally, students shall take all reasonable care to protect their personal information while using social networking technologies.

Commercial Use

- Commercial use of NNPS computing systems by students is prohibited.

Violations may result in a loss of access as well as other disciplinary or legal action.

Reference School Board Policy and Procedures IJND for the complete Technology Acceptable Use Policy.

The Parent/Legal Guardian may withdraw permission by providing written notice to the school.