

**COMPUTER NETWORK AND INTERNET  
ACCEPTABLE USE POLICY AND AGREEMENT**

**Agreement Form**

(Every user, regardless of age, must read and sign below):

I have read, understand and agree to abide by the terms of the foregoing Acceptable Use Policy and Agreement. Should I commit any violation of in any way misuse my access to the Newark City Schools' computers, computer network, and/or the Internet, I understand and agree that my access privilege may be revoked and disciplinary action may be taken against me as outlined in the applicable Handbook or Code of Conduct.

(Please Print Clearly)

Name \_\_\_\_\_ Home Phone \_\_\_\_\_

User Signature \_\_\_\_\_ Date \_\_\_\_\_

Student Age \_\_\_\_\_ Student Grade \_\_\_\_\_ Student ID (if known) \_\_\_\_\_

If am signing the Policy and Agreement when I am under 18, I understand that when I turn 18, this Policy and Agreement will continue to be in full force and effect and I agree to abide by this Policy and Agreement.

**Parent or Guardian Network Usage Agreement**

(To be read and signed by parents or guardians of student who are under 18)

As the parent or legal guardian of this student, I have read, understand and agree that my child or ward shall comply with the terms of the Newark City Schools' Acceptable Use Policy and Agreement for user access to the Newark City Schools' computer, computer network, and Internet. I understand that access is being provided for educational purposes only. However, I also understand that it is impossible for the Newark City Schools to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by the Policy and Agreement. I am therefore signing this Policy and Agreement and agree to indemnify and hold harmless the Newark City Schools that provides the opportunity to the Newark City Schools' students for computer network and Internet access against all claims, damages, losses and costs, of whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the foregoing Policy and Agreement. Further, I accept full responsibility for supervision of my child's or ward's use of his or her access account if and when such access is not in the school setting. I hereby give permission for my child or ward to use the building-approved account to access the Newark City Schools' computers, computer network, and Internet.

(Please Print Clearly)

Parent/Guardian Name \_\_\_\_\_ Phone \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

Address \_\_\_\_\_

## STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY PERSONAL RESPONSIBILITIES

### Personal Responsibility

By signing this Policy and Agreement, you are agreeing not only to follow the rules in this Policy and Agreement, but are agreeing to report a misuse of the network to your immediate teacher, supervisor, or director. Misuse means any violations of this policy, Board of Education Policy, or any other use that is not included in the policy, but has the effect of harming another or his or her property.

### Term of the Permitted Use

**A properly signed and submitted copy of this document is required to have a computer account activated for the given school year. Please sign and return the Acceptable Use Agreement which is included in your packet.**

## STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board provides Education Technology so that students can acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board of Education provides students with access to the Internet for limited educational purposes only and utilizes online educational services to enhance the instruction delivered to its students. The District's Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

This policy and its related administrative procedures and the Student Code of Conduct govern students' use of the District's personal communication devices (such as, computers, laptops, tablets, e-readers, cellular/mobile telephones, smartphones, and any other web-enabled device), when connected to the District's network, the District's Internet connection, and online educational services ("Education Technology" or "Ed-Tech").

Users have no right or expectation to privacy when using the Ed-Tech (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the network and Internet).

First, and foremost, the Board may not be able to technologically limit access to services through its Education Technology to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources which may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures, which protect against (e.g. filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the

Board or the Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the Education Technology, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or Technology Director may temporarily or permanently unblock access to websites or online educational services containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

Parents are advised that a determined user may be able to gain access to services and/or resources on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents may find inappropriate, offensive, objectionable or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

Pursuant to Federal law, students shall receive education about the following:

- A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications
- B. the dangers inherent with the online disclosure of personally identifiable information
- C. the consequences of unauthorized access (e.g., "hacking") "harvesting", "digital piracy", etc.), cyberbullying and other unlawful or inappropriate activities by students via any form of electronic communication , and
- D. unauthorized disclosure, use, and dissemination of personal information regarding minors

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the Education Technology. Such training shall include, but not be limited to, education concerning appropriate use of any form of electronic communication, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. All Internet users (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy.

Students and staff members are responsible for good behavior on the Board's computers/network and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not sanction any use of the Education Technology that is not authorized by or conducted strictly in compliance with this policy.

Students shall not access social media for personal use from the District's network, but shall be permitted to access social media for educational use in accordance with their teacher's approved plan for such use.

Users who disregard this policy may have their use privileges suspended or revoked, and disciplinary action taken against them. Users of the Board's Education Technology are personally responsible and liable, both civilly and criminally, for uses of the Ed-Tech not authorized by this Board policy.

The Board designates the Superintendent and Technology Director as the administrators responsible for initiating, implementing, and enforcing this policy as they apply to students' use of the District's Education Technology.

### **USE OF PERSONAL COMMUNICATION DEVICES**

“Sexting is prohibited at any time on school property or at school functions. Sexting is the electronic transmission of sexual messages or pictures, usually through cell phone text messaging. Such conduct not only is potentially dangerous for involved students, but can lead to unwanted exposure of the messages and images to others, and could result in criminal violators related to the transmission or possession of child pornography. Such conduct will be subject to discipline and possible confiscation of the PCD.