Book	Policy Manual
Section	(Series 4000-4999) INSTRUCTION
Title	Student Acceptable Use of Technology
Code	4526.1
Status	Active
Adopted	June 25, 2019

Rye City School District
Rye, New York

4526.1

Student Acceptable Use of Technology

The Rye City School District strives to provide its community with an abundance of opportunities to learn, use, and apply the 21st century technology skills necessary to be successful collaborators in an ever more digital society. To that end, the District strives to provide all educators with ongoing, sustainable and structured staff development that meaningfully integrates technology across all learning environments. The District considers access to a computer Network, including the Internet, to be the most essential and transformational tool it can provide to enhance education, research, communication and collaboration. Through the use of the District Network, students may access a variety of web-based resources, applications, and platforms, participate in global communication, and utilize powerful tools for successful and meaningful learning and collaboration across curricula. To ensure the proper use of technology, the District's Acceptable Use Policy (AUP) contains guidelines for access to, and use of, technology. All students in the District and their parent(s)/guardian(s) must review, agree to abide by, and sign the AUP annually.

When an individual accesses computers, computer systems, and/or computer networks including the Internet provided by the District (hereinafter the District's computer resources"), he/she assumes certain responsibilities and obligations. Access to the District's computer resources is subject to federal, state and local law, as well as District policies including this one. The use of the District's computer resources is a privilege, not a right, and inappropriate use will result in the cancellation of privileges and/or disciplinary action by District officials.

With increased concern about identity theft, unwarranted invasion of privacy, and the need to protect personally identifiable information, prior to students being permitted by staff to use any cloud-based educational software or application outside of the District Network/domain, staff must obtain approval from the District's Director of Technology. The Director of Technology will review all such software/applications and their privacy policies to determine if a formal contract and/or parental permission is required or if the terms of service are sufficient to address privacy and security requirements. Certain software/applications identified by the District, such as Google Apps for Education, may not be used by students unless their parents sign a separate consent form provided by the District in accordance with the appropriate District policies and legal requirements.

Educational Purpose

The pursuit of educating responsible digital citizens, in an ever increasingly technologically demanding society, is a primary goal for students of the Rye City School District. Expectations for technology including online/Network behavior should translate to all school situations and settings similar to appropriate behaviors outlined as part of the District Code of Conduct. To that end, the following rules have been written to promote positive, effective digital citizenship among students and staff.

District Network

The Rye City School District provides students access to the District's computer "Network" to maximize educational opportunities and resources. This Network includes Internet access, wireless Internet access, computer services, computer

equipment, and related equipment for educational purposes.

- Student access to technology in school is a privilege, not a right, and it may be suspended or restricted.
- It is the expectation of the District that all access to the Internet while on school property shall be through the authorized District Network login.
- The District will notify parents about policies governing the use of the District Network. Students shall only be permitted to utilize the District's Network while on school property, after submitting a completed and signed Acceptable Use of Technology Agreement Form. The Acceptable Use of Technology Agreement Form must be signed by parent(s)/guardian(s) and students at the start of each school year, manually or electronically.
- The District has the right to place reasonable restrictions on the material that students search, access and/or post through the Network.
- Students shall follow the rules set forth in the District Code of Conduct as well as state and federal laws such as the Family Educational Rights and Privacy Act (FERPA), the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), and others as appropriate.

Internet Filtering

Internet filtering technology on the Network is used to prevent access to material that is obscene, illegal (i.e., child pornography) and/or harmful to minors, as defined by the Children's Internet Protection Act (CIPA). This filtering applies to Internet access through the use of District computers as well as the use of personal wireless devices. Students are prohibited from attempting to tamper with or circumvent such filtering.

Student Internet Access

- Students may obtain access to the Internet, including wireless Internet access, with the approval of their parent(s)/guardian(s) and the school when permitted by a staff member. Each student and his/her parent(s)/guardian(s) must sign an Acceptable Use of Technology Agreement Form to be granted individual access to the District's Network and wireless service.
- In order to access the Internet, students must use the District's network.
- Students in grades 9-12 are permitted to participate in the Rye High School Bring Your Own Device ("BYOD") program. Permitted "personal electronic devices" include but are not limited to personal laptops, smart phones, portable storage media, all recording devices, all Internet connected devices, and handheld devices such as iPods and iPads. With classroom teacher approval, students may use their own devices to access the Internet for educational purposes. All such devices used with the District's computer resources are subject to review by the District's Director of Technology, or individuals/entities designated by the Superintendent of Schools, if there is reason to suspect that the device is causing a problem to the District's computer resources. The District reserves the right to monitor, inspect, and/or confiscate personal electronic devices when administration has reasonable suspicion that a violation of this policy or other District policies has occurred.
- If students bring their own personal electronic device(s) to school, they shall take all reasonable measures to protect against theft or damage of such wireless devices. Students assume full responsibility for the device(s). The District will not be liable for the loss, damage, theft, or misuse of any personal electronic device(s) brought to school. The District will bear no responsibility nor provide technical support, troubleshooting, or repair of electronic devices owned by anyone other than the District.
- Students utilizing the District's wireless Internet service shall be permitted to log in with one (1) wireless device at a time.
- All users will be prohibited from accessing Social Networking Sites through the District Network without appropriate District and/or parental consent. Social Networking Sites (SNS) are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the School District community which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, blog sites, etc.).
- Students in grades 6-12 will have individual email addresses provided by RCSD. All email communication between staff and students must occur within the RCSD domain.
- Students under the age of 13 may not access anything outside of the RCSD Network and/or domain.

Acceptable Use and Conduct

- Access to the District's computer Network is provided for educational purposes and research consistent with the District's mission and goals.
- All Network users will be issued an account, login name, and password. Passwords must be changed periodically and not shared with other users.
- All users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to access their accounts. Users will be held responsible for any policy violations that are traced to their accounts. Under no conditions shall a user provide his/her password to another person.
- Network users identifying a security problem on the District's Network must notify the appropriate teacher, administrator, or the Director of Technology. Under no circumstances should the user demonstrate the problem to anyone other than to the District official or employee being notified.
- Any Network user identified as a security risk or having a history of violations of District computer use guidelines may be denied access to the District's Network.
- Students may use technology equipment provided by the District or personal wireless devices.

Prohibited Activity and Use

The following is a list of prohibited activity concerning use of the District's computer Network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the District's Network or Internet. Violations constituting crimes may be referred to law enforcement. Violations include but are not limited to:

- Accessing or attempting to access the District's computers, Network, Internet, or software or applications without the appropriate District and/or parent authorization or beyond the limits of such authorization.
- Utilizing the District's computer resources including Network and Internet to access, create, download, edit, view, store, send or print material that is illegal, offensive, threatening, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the District is prohibited. A special exception to certain sensitive materials for projects may be made for literature if the purpose of such access is to conduct research and the access is approved by the teacher or administrator. The District's determination as to whether the nature of the material is considered offensive or objectionable is final. The District will respond to complaints of harassing or discriminatory use of the School District's computer resources in accordance with Policy 0100 (Equal Opportunity), Policy 0110 (Sexual Harassment) and/or Policy 5040 (Dignity for All Students Act).
- Revealing or posting the personal address, telephone number, photograph, video, recording, or other personal information of oneself or another person without the appropriate District and parental consent.
- Infringing on any copyright or other intellectual property, including copying, installing, receiving, transmitting or making available any copyrighted software on the District computer Network.
- Violating the rights of copyright owners and/or plagiarizing information found on the Internet.. The source of online research information should always be cited. If students are unsure whether or not they can use research found online, they should ask their teacher.
- Using or attempting to use another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (email) of other system users, or deliberately interfering with the ability of other system users to send and/or receive email.
- Forging or attempting to forge e-mail messages.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing software to District technology, including any downloads, games, hacking tools, music sharing or video sharing applications or others or attempting to run such software from a personal device such as a thumb/flash drive or any other media/device without the permission of the appropriate District official.
- Accessing, modifying or deleting others' files or system settings without express permission. Tampering of any kind is strictly forbidden.
- Deliberately attempting to tamper with, circumvent filtering or access, or degrade the performance of the School District's computer resources or to deprive authorized users of access to or use of such resources.
- Engaging in vandalism. Vandalism is defined as malicious attempt to harm or destroy District equipment or materials, data of any user of the District's Network or of any of the entities or other Networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing computer viruses on the Network.
- Damaging School District technology in any way.
- Stealing data, equipment, or intellectual property.
- While on school property, accessing the Internet via the District Network without the supervision of a teacher or staff member.
- Remotely accessing the District's Network.
- Using technology to engage in attacks on the District's Network and/or Internet, intentionally disrupt Network traffic, or "crash" the Network and/or connected systems.
- Student recording of classroom instruction without the express permission of the teacher.
- Engaging in any illegal acts, such as computer fraud, threatening the safety of self or others, hacking, arranging for a drug sale, purchasing alcohol, or engaging in any activity that violates local, state, or federal laws.
- Using the Network in a fashion inconsistent with directions from teachers and other staff and generally accepted Network etiquette.

Personal Safety

The District takes great measures to protect the personal safety of all its Internet users. The District performs thorough reviews of all computer software and Internet application Privacy Policies, and obtains parental consent when deemed necessary or appropriate by the District's Director of Technology or his/her designee, prior to granting students and/or staff access to anything outside of the District domain. The District supports The Student Privacy Pledge initiative site committed to following existing federal law and regulatory guidance regarding the collection and handling of student data. The Student Privacy Pledge is taken by service providers that are committed to protecting the information of their users. Specific policies referenced in The Student Privacy Pledge include, but are not limited to, The Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA).

- Students will not post, on any forum/platform, personal contact information about themselves and/or other people. Personal contact information may include, but is not limited to, a name, e-mail address, telephone number, image, home phone and/or address, school name and/or address, or anything that personally identifies a student.
- Students/parent(s)/guardian(s) will promptly disclose to a teacher or other school employee any messages and/or images viewed and/or received that they feel is inappropriate or makes them feel uncomfortable. If a student mistakenly accesses inappropriate information, he/she should immediately tell a teacher or another District employee.
- Students should never agree to meet with anyone encountered online.

System Security

- Students are responsible for their individual access account.
- Students should not distribute and/or share computer passwords with anyone.
- Students should immediately notify a teacher and/or staff member if they see or hear about a possible security threat and/or problem.
- Students will not attempt to access websites blocked by the District, including the use of chat rooms, social media sites, and/or personal email to purchase items online.
- Student may not attempt to circumvent or subvert the security provisions of any District computer, Network, or other technology system.
- Students may not remove or relocate District-owned computer resources without the prior authorization from the District's Director of Technology or his/her designee.

Monitoring and Regulating Technology Use

- The District's computer resources, including all telephone and data lines, are the property of the District. The District reserves the right to access, view, or monitor any information or communication stored on or transmitted over the Network, or on or over equipment that has been used to access the District's computer resources. There is no guarantee of privacy associated with an individual's use of the District's computer resources. Users should not expect that e-mail, voice mail or other information created or maintained in the system (even those marked "personal" or "confidential") are private, confidential, or secure.
- Students' personal files on the District system and records of their online activity are not private and may be monitored by the District and result in appropriate discpline.
- Personal wireless devices may be seized and inspected on school grounds, in accordance with Section 5300.65 in the District Code of Conduct.
- If it is believed that a student has violated this Acceptable Use Policy, parent(s)/guardian(s) will be contacted. If discipline is being imposed, the student and parents will be provided with the due process in the manner set forth in the District Code of Conduct.
- As a result of any violations of this policy, additional restrictions may be placed on a student's use of the Network and/or other computer resources. A student's privilege of using the such Network and computer resources may be revoked by the District at any time.
- All users of the District's Network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The District reserves the right to control access to the Internet for all users of its computer resources. The District may either allow or prohibit certain kinds of online activity, or access to specific websites. Incidental personal use of the District's computer resources must not interfere with the District community's ability to use the resources for professional and academic purposes nor violate other District policies or law.

Disclaimer

The Rye City School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by, or through, the system will be error-free and/or without defect. The District shall not bear any liability for any damage users may suffer including, but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District shall not bear any liability for financial obligations arising through the unauthorized or illegal use of the Network or District computer resources. The District shall not be held liable for the content already existing on student personal wireless devices including but not limited to music, movies, pictures, games, etc.

The District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the user's own negligence or the errors or omissions of any user.

Users are responsible for any financial costs, liabilities, or damages incurred by the School District as a result of improper use of School District technology, including, but not limited to, equipment (including repairs), replacement of and/or insurance for Chromebooks or other School District issued technological devices, legal fees, and other costs.

References:
5040, Student Harassment and Bullying Prevention under the Dignity for All Students Act (DASA)
5300, Code of Conduct
Family Educational Rights and Privacy Act (FERPA)
Children's Internet Protection Act (CIPA)
Children's Online Privacy Protection Act (COPPA)

The Electronic Communications Privacy Act (ECPA)
The Computer Fraud and Abuse Act (CFAA)
The Student Privacy Pledge (https://studentprivacypledge.org/signatories/)
The Future of Privacy Forum (FPF)
The Software & Information Industry Association (SIIA)
Adoption Date: January 24, 2012
Revised Regulation Adoption Date: July 22, 2014
Revised Regulation Adoption Date: July 1, 2016
Revised Policy Adoption Date: April 10, 2018
Revised Policy Adoption Date: June 25, 2019
Effective Date: July 1, 2019

Rye City School District Acceptable Use Policy Agreement

I understand and will abide by the provisions and conditions of the District's Acceptable Use Policy. I understand that any violations of the above provisions may result in disciplinary action, the revoking of my user account, and appropriate legal action. As a condition of Network use, I am obligated to report any use of the District technology systems in a manner inconsistent with or in violation of the terms and conditions listed above. I understand that I may be provided additional consent forms that must be signed in order for student to use or access certain cloud-based educational software or applications outside of the District domain, including but not limited to Google Apps for Education. If consenting to this Agreement electronically, I agree that my electronic signature is the legal equivalent of my manual (hand-written) signature.

Student Name _____

Parent/Guardian Name _____

Student Signature _____

Parent/Guardian Signature _____

School _____

Date _____