4525 INFORMATION TECHNOLOGY USAGE

I. PURPOSE

It is the policy of the Board of Education to offer employees, students and other authorized individuals access to a variety of information technology resources, including computer workstations, laptops, tablets, wired and wireless local area networks, wide area network, and the Internet.

II. SCOPE

1. The Superintendent of Schools shall designate a Director of Information Technology to oversee the District's computer network and assets.

2. The Director of Information Technology and his/her staff shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.

3. All signed staff and student agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district IT Office. Logs shall be kept of any acceptance of the Acceptable Use Policy via electronic means (e.g. Click through pages).

III. GENERAL STATEMENT OF POLICY

The purpose of Rensselaer City School District information technology resources is to advance the school district's educational mission. The policies of the school as related to Acceptable Information Technology Usage are intended to address issues that impact this broad scope of technological resources including school network systems, the internet and other forms of technology that may emerge in future years.

The use of the school district information technology resources and access to use of the Internet is a privilege, not a right. Unacceptable use of the school district information technology resources or circumvention, whether attempted or successful, of established information security measures, including the district web filter, antivirus or security policies may result in one or more of the following consequences: suspension or cancellation of use or access privileges; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws. The consequences will depend on the nature and degree of the violation and the number of previous violations.

As information technologies advance and internet use increases, modifications will have to be made to the District's specific IT policies and procedures. However, the basic requirements of the policies and procedures will not change.

IV. AUTHORIZED USERS

Authorized users are: (1) faculty, staff, and students of the Rensselaer City School District; (2) others whose access furthers the mission of the school and whose usage does not interfere with other users' access to resources. In addition, a user must be specifically authorized to use a particular computing or network resource by the individual responsible for operating the resource.

V. USE OF IDS AND PASSWORDS:

The Director of Information Technology is designated by the district as the individual responsible for identifying standards for access for the use of information technology resources. This standard identifies the minimum password requirements to protect school data and systems. It applies to all electronic devices and systems connected to the school network including, but not limited to computers, network switches and routers, personal computing devices, laptop computers, password authenticated software, etc.

Required characteristics of passwords:

- A password or passphrase or other strong authentication must be used for all devices supporting authentication and password authenticated software connected to the school network.
- A password or passphrase must be seven characters long.
- Passwords or passphrases may need to be changed every 180 days as required by each system, but all passwords or passphrases will be changed at least annually.
- A password or passphrase must be complex and include a combination of character types such as numbers, special characters, lower case letters, upper case letters, non-keyboard characters to help protect against automated cracking.
- Do not share the password assigned or established by you. Each individual in whose name an access account is issued is responsible at all times for its proper use.

- Use of computer resources by other than the logged on user is not allowed. Users should not log on with their credentials to any system for another person. If access to a system is needed, a helpdesk ticket should be submitted requesting access.

- Sharing of passwords or passphrases is considered an unacceptable use of the School District information technology resources.

- Shared username and passwords designated by the Director of Information Technology shall be allowed only in specific circumstances, such as online testing sessions. These accounts should be disabled when not in use.

- Adherence to password requirements will be reviewed as part of the normal School Internal Audit procedures.

VI. USE OF INFORMATION/DATA:

Users of the technology resources should take care to protect the integrity and sensitivity of data accessed on the school's network. Users should:

1. Access only accounts, files and data that are your own, that are publicly available, or to which you have been given authorized access. Secure information that is in your possession.
2. Maintain the confidentiality of information classified as private, confidential.
3. Use school information for tasks related to job responsibilities and not for personal purposes.
4. Never disclose information to which you have access, but for which you do not have ownership, authority, or permission to disclose.
5. Access to some applications and internet resources has been restricted by blocking and filtering hardware and software. Unauthorized use of equipment, attempting to access intentionally blocked websites or making modifications to equipment/software by any means, is prohibited. If modifications to equipment/software are required, appropriate district personnel should be contacted to obtain technical assistance.
6. The implementation of security policies and content filtering does not alleviate the responsibility of Staff members to monitor the network/internet activities of students under their supervision.
7. Users will notify the IT Department if a security problem is identified.
8. 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.

VII. Prohibited Activity and Uses

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 network.

1. Using the network for commercial activity, including advertising.
2. Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
3. Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
4. Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
5. Using another user's account or password.
6. Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
7. Forging or attempting to forge e-mail messages.
8. Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another 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 a computer virus on the network.
9. Using the network to send anonymous messages or files.
10. Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
11. Revealing the personal address, telephone number or other personal information of oneself or another person.
12. Intentionally disrupting network traffic or crashing the network and connected systems.
13. Installing personal software or using personal disks, hard drives, or USB flash drives on the district's computers and/or network without the permission of the appropriate district official or employee.
14. Using district computing resources for commercial or financial gain or fraud.
15. Stealing data, equipment or intellectual property.
16. Gaining or seeking to gain unauthorized access to any files,

resources, or computer or phone systems, or vandalize the data of another user.

17. Wastefully using finite district resources.
18. Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
19. Using the network while access privileges are suspended or revoked.
20. Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

VIII. USE OF PERSONALLY OWNED DEVICES

1. Staff and students may use a personally-owned device , or “Bring Your Own Device” (BYOD) for internet access only under the following stipulations:

a. Device may be used only to access internet resources via the RCSD Wireless LAN. BYOD devices shall not be connected to the Wired LAN. Attempts to access other network resources (i.e. file on local servers) is prohibited. Access to District cloud based information systems, including email, student information systems, district provided storage and applications is allowed, provided the user has been granted access and has a valid username/password.

b. All BYOD devices must have current system updates and antivirus software.

c. Students must obtain parental permission to connect personal computing devices to the RCSD Wireless Network. The IT Department will control this through the use of policies and permissions granted to students who have returned the RCSD Internet Safety Policy signed by a parent or guardian. Connection of devices by using credentials belonging to someone else is strictly prohibited and will result in Disciplinary action. All provisions of this policy remain in effect while accessing the internet via BYOD devices.

VIII. STUDENT EMAIL ACCESS

1. Use of personal email by students is not permitted.

2. Use of District provided email for educational uses is allowed. Communications shall be limited to within the District's email system (Student-Student, Student-Teacher, Teacher-Student) except where

authorized by the Director of Information Technology (eg College applications, Distance Learning, collaboration with other schools).

3. Students shall complete a course in digital literacy and internet safety prior to being given access to email, typically in 5th Grade.

4. Email, both sent and received, is archived, filtered and monitored. Any email containing inappropriate language or content will be rejected and flagged as such for review.

5. Email for students is considered a privilege and accounts can be suspended or terminated at the discretion of the administration and Director of Information Technology.

VI. CONFIDENTIALITY AND PRIVACY

1. Authorized access to data or information entails both privilege and responsibility, not only for the user, but also for the system administrator. In general, the school will treat information stored on computers as confidential. However, there is no expectation of privacy or confidentiality for documents and messages stored on school-owned equipment. Additionally, e-mail and data stored on the school's network may be accessed by the school for the following purposes:

    a. troubleshooting hardware and software problems,

    b. preventing unauthorized access and system misuse,

    c. retrieving business/program related information,

    d. investigating reports of violation of this policy or local, state or federal law,

    e. complying with legal requests for information,

    f. re-routing or disposing of undeliverable mail.

2. The District's network is monitored. The user understands that there is no expectation of privacy on the District's computers either through e-mail, any network services, individually created files or browsing history, and that they are responsible for the content of those files and information disclosed or exchanged.

3. By authorizing use of the school district information technology resources, the school district does not relinquish control over materials

on the system, or materials contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

4. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law. An individual search may be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

5. School district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery.

6. The school district will cooperate fully with local, state and federal authorities in any investigation concerning, or related to, any illegal activities not in compliance with school district policies conducted through the school district system.

VII. SANCTIONS AND TAKING DISCIPLINARY ACTION

Users in violation of this policy are subject to the full range of sanctions, including the loss or suspension of computer or network access privileges without notification, appropriate disciplinary or legal action. Some violations may constitute criminal offenses, as outlined in state and federal statutes; the school will carry out its responsibility to report such violations to the appropriate authorities. The network administrator shall have the authority to deny access, for unauthorized use, to the school's computers and network systems under their control.

In the event that that school's policy for Information Technology Usage is violated, disciplinary action may be taken in accordance with the following: standards for student conduct; the appropriate employment agreement; or the appropriate bargaining agreement.

Unacceptable use of information technology resources includes:

1. Providing, assisting in, or gaining unauthorized or inappropriate access to the district's technology resources, including any type of voice, video or data information server;
2. Activities that interfere with the ability of students/staff members to use the district's technology resources or the network connected services effectively;
3. Activities that result in the loss of another student/staff member's work or unauthorized access to another student/staff member's

work; activities that result in the disabling of another user's account by anyone other than IT department personnel.

4. Distribution of any material in such a manner that might cause congestion of the voice, video, and data networks.
5. Distribution or collection of obscene, abusive or threatening material via telephone, video, electronic mail, internet or other means;
6. Use of technology resources for a commercial, political, or profit making enterprise, except as specifically agreed to with the district;
7. Use of technology system to engage in any illegal act or violate any local, state or federal statute or law;
8. Use of the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation;
9. Use of the school district system to post private information about another person or to post personal contact information about themselves or other persons.

VIII. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district information technology resources is at the individual's own risk. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The School District will not be responsible for financial obligation arising through unauthorized use of School District resources or the internet.

IX. NOTIFICATION

All individuals shall be notified of the school district policies relating to Acceptable Information Technology Resources Usage. This notification shall include the following:

1. Notification that information technology use is subject to compliance with school district policies.
2. Disclaimers limiting the school district's liability relative to:
   - Information stored on any storage media provided by or owned by the school. This would include diskettes, hard drives, thumb drives servers or any other medium developed at a future point in time.

- Information retrieved through school district computers, networks or on-line resources.

- Personal property that may be damaged when accessing school district computers, networks or on-line resources.

- Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed internet accounts.

4. Notification that, even though the school district may use technical means to limit a users Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a user through the Internet is the sole responsibility of the user or the user's parents / guardians in the case of a student.

6. Notification that should the user violate the school district's policy for Acceptable Information Technology Resources Usage, the individual's access privileges may be revoked or suspended[1] and that, disciplinary action may be taken and/or appropriate legal action may be taken.

7. Notification that all provisions of the usage policy are subordinate to local, state and federal laws.

X. FOR STUDENTS OF RENSSELAER CITY SCHOOL DISTRICT - PARENT RESPONSIBILITY

1. Outside of school, parents / guardians bear responsibility for the same guidance of internet use as they exercise with information sources such as television, telephones, radio, movies and other possible offensive media.

2. Parents or guardians will be notified that their student(s) will be using school district resources/accounts to access the internet, and must notify the district in writing if their student is not to have access to the internet or e-mail using school resources.

XI. INTERNET USE AGREEMENT

1. The proper use of the internet, and the educational value to be gained from proper internet use, is the joint responsibility of students, parents/guardians and employees of the school district.

2. For Students of Rensselaer City School District:

   - This policy requires the permission of and supervision by, the school's designated professional staff before a student may use a school account or resource to access the internet.

   - Parents must notify the district, in writing, if their student is not to have internet or e-mail access.

   - Students will be instructed in the appropriate use of the Internet, including the use of e-mail by classroom teachers and/or media specialists prior to independent use of the Internet.

3. The Internet Use Agreement form must be read and signed by users in 7th Grade and above. For Elementary School users, Parents shall read the Internet Use Agreement and sign the parental permission sheet.

4. Independent use of the Internet refers to a student, or group of students, using a computer to access the Internet or send e-mail.

XII. OTHER ISSUES:

The network administrator should devise plans that will ensure the following issues have been addressed:

1. <u>Physical Access:</u>

   - Physical access to network servers and computer workstations must be restricted as much as possible. Server rooms must be secured by a lock and be safe from fire and water damage.

   - Workstations not in use for extended periods (e.g. at night and on weekends) must be turned off.

   - Laptops or notebook computers should be physically restrained (e.g. via an anchoring device or inside a locked cabinet or cart).

   - Password protected screen saver programs should be used and set to engage in 15 minutes or less for computers that are left unattended or are in open locations. Exceptions to this are Kiosk

computers setup for maximum availability of a single application (e.g. Card Catalog PCs)

2. Monitoring: Financial systems must be capable of generating access logs and exception reports. Regular review of these reports should be performed by the system administrator.

3. Inactive Accounts: When a user is no longer authorized to access the technology resources of the school district, their account should be disabled promptly. Supervisors should immediately notify the IT Department when users no longer need access to a system or are no longer employed by the District. IT Department shall conduct periodic audits of all systems to ensure inactive accounts have been disabled or deleted.

4. Disaster Recovery: The District shall develop and maintain a formal disaster recovery plan for the information technology (IT) system. This plan should outline the precautions to be taken to minimize the effects of a disaster, and allow the District to either maintain, or quickly resume, mission-critical functions. The plan should be distributed to all responsible parties, periodically tested and updated as needed.

5. Backups: Periodic backup copies of software and data must be made, tested, and stored securely (not in staff cars, homes, etc). The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems. Users that store data on local drives must ensure that the data is backed up as frequently as necessary to prevent a disruption; no less than on a weekly basis. Back-up copies of data should be stored at secure offsite locations.

6. Segregation of Duties: (Users of Financial Applications) Rights and privileges assigned to users of financial applications are to be consistent with the roles and responsibilities of each individual user. These rights and privileges are to be assigned by the network administrator responsible for the financial applications. Periodic reviews of user activity logs should occur to ensure that access to sensitive data is consistent with assigned roles. In cases where electronic signatures are used, the school should take all means necessary to ensure that the electronic signature is password-protected and is used only by individuals that have been authorized by the board of education.

7. Firewall or filtering: A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to limit network access to the device storing private data.

8. Anti-virus technology: Desktop and laptop computers must have anti-virus software or filters installed and updated on a systematic and routine basis (automatic updates are recommended). In addition, other Windows computers, including servers, must have antivirus software installed and updated daily.

9. Disposal of data and equipment: Either a "secure deletion" program must be used to erase data from hard disks and media prior to transfer or disposal of hardware or a Certificate of Destruction must be obtained from the electronics recycling vendor. Permanent media (e.g., CD's, etc) must be physically destroyed.

Adopted: January 10, 2006
Revised: June 24, 2008
Revised: June 11, 2014
Revised: January 27, 2016