EHA

ROCHESTER SCHOOL DISTRICT COMPUTER & COMMUNICATIONS POLICY STATEMENT

Introduction

The Rochester School Board recognizes the value of computer and other electronic resources to improve student learning and enhance the administration and operation of its schools. To this end, the Board encourages the responsible use of computers, computer networks, including the Internet, and other electronic resources, in support of the mission and goals of the Rochester School Department and its schools

Because the Internet is an unregulated, worldwide vehicle for communication, information available to staff and students is impossible to control fully. Therefore, the Board adopts this policy governing the voluntary use of electronic resources and the Internet in order to provide guidance to individuals and groups obtaining access to these resources on School Department-owned equipment, School Department-affiliated organizations, and personal devices.

Policies, guidelines and rules refer to all computing devices including but not limited to computers, mobile web enabled devices, iPads, MP3 players, portable memory storage devices, calculators with interfacing capability, cell phones or ECDs (electronic communication devices), digital cameras, etc., as well as technology infrastructure, associated peripheral devices and/or software.

Policies, guidelines, and rules refer to any computing or telecommunication devices owned by, leased by, in the possession of, or being used by students and/or staff that are operated on the grounds of any district facility or connected to any equipment at any district facility by means of web connection, direct connection, telephone line or other common carrier or any type of connection including both hardwired, fiber, infrared and/or wireless.

This Technology Acceptable Use Policy also applies to any online service provided directly or indirectly by the district for student use, including but not limited to: Google Apps for Education accounts, Email, Calendar, and Infinite Campus (Parent/Student Access to Student Information System).

School Department Rights and Responsibilities

It is the policy of the Rochester School Board to maintain an environment that promotes ethical and responsible conduct in all computer and communications equipment activities by staff and students. It shall be a violation of this policy for any employee, student, or other individual to engage in any activity that does not conform to the established purpose and general rules and policies of computer/communications equipment use. Within this general policy, the School Department recognizes its legal and moral obligation to protect the well being of students in its charge. To this end, the School Department retains the following rights and recognizes the following obligations:

1. To monitor the use of computer network and the communications network activities. This may include real-time monitoring of Internet access and/or maintaining a log of Internet activity, or attempted activity, for later review.

2. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to School Department owned equipment and, specifically, to exclude those who do not abide by the School Department's acceptable use policy or other policies governing the use of school facilities, equipment, and materials.

3. To restrict on-line destinations, including in-coming signals, through software or other means.

4. To remove a user's access, a device, or connection to the network that is not approved and secure.

5. To provide guidelines and make reasonable efforts to train staff and students in acceptable use and policies governing on-line, wide-area, and local use of computers and communication equipment.

6. Prior to allowing user access, a signed statement of compliance will be executed, certifying that the user understands and agrees to comply with Rochester School District policy.

7. School district reserves the right to "block" at any time any sites or services that could cause bandwidth issues that affect the overall stability of the network.
8. The district may establish a retention schedule for the removal of e-mail. The district makes a best effort to retain email for 90 days.
9. Guests/Contractors are not automatically eligible for a district e-mail account. Email or network access accounts may be granted if directly sponsored by a district administrator and approved by the Superintendent or designee.

The Superintendent or designee shall develop and implement administrative procedures that ensure students are educated on network etiquette and other appropriate online behavior, including: interaction with other individuals on social networking web sites and Cyberbullying awareness and response.

Staff Responsibilities

1. Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the Rochester School District.
2. Staff should make reasonable efforts to become familiar with the Internet and its use so that effective monitoring, instruction, and assistance may be achieved.
3. Ensure all student and non-school system users are informed of the district's electronic communications policy and administrative regulations. All such agreements will be maintained by the school office or as part of the student agenda. All students using **Google Apps for Education** must have a signed permission form.

User Responsibilities

Use of the computer and communication equipment provided by the School Department is a privilege that offers a wealth of information to improve research and productivity. Where it is available, these resources are provided to staff, students, and other patrons at no cost. In order to maintain the privilege, users agree to learn and comply with all of the provisions of this policy.

1. The School Department reserves the right to monitor, review, and copy any communications at any time.
2. Failure to report breaches of this policy is itself a violation.
3. Users will be individually responsible for their own behavior and violation of this policy may result in discipline actions in the form of written reprimand, suspension, expulsion, termination of employment, or others forms decided by the school board and superintendent.
4. Staff will be responsible for maintaining their own systems for reliability, integrity, availability, and for physical protection.
5. Disciplinary or legal action including, but not limited to, criminal prosecution under appropriate local, state, and federal laws. Violation of local, state, and federal laws will be reported to the proper enforcement authorities.
6. By accessing the district's Internet, computers and network resources, users acknowledge awareness of the provisions of this policy, and awareness that the district uses monitoring systems

to monitor and detect inappropriate use and may use tracking systems to track and recover lost or stolen equipment. (Chromebooks, iPads)

7. Users are responsible for the use of their individual access account(s) and should take all reasonable precautions to prevent others from being able to use their account(s), including coworkers, friends or family.

Acceptable Use

1. All use of the computer and communications equipment must be in support of educational and research objectives consistent with the mission and objectives of the School Department.
2. Proper codes of conduct in electronic communication must be used. All users are representing the Rochester School District and must use polite and respectful language in any dealings through this equipment.
3. Use network etiquette, being polite and using network resources in a safe and legal manner.
4. Use of the network is a privilege, not a right.
5. Confidential information will be sent under a secure medium.
6. Protect your own data.
7. Use extreme caution to verify messages go to the correct address/user.
8. Any software/hardware must be pre-approved by the CIC Staff.
9. Immediate notification to CIC Staff of a system compromise (Virus, Trojan, hackers, unauthorized access, etc.).

Use of Home/Personal equipment or software can only be used on BYOD (Bring Your Own Device) network or as stand-alone devices. The school district assumes no liability for personal equipment and services.

Unacceptable Use

Prohibited activities include, but are not limited to, the following:

1. Users will not obtain, or provide to others, illicit copies of copyrighted software or documents. Only software provided by or approved by the Rochester School District may be installed on a School District computer. Users will not download or install software, or upgrades to approved software already installed, unless directed to do so by the Superintendent or his designee(s). Users will not download or install any unauthorized software, including freeware and shareware, on School District computers.
2. Users will not use the computer network to attempt to gain unauthorized access to any computer or communications system.
3. Users will not use the computer or communications equipment to give out <u>any</u> personal information about another person.
4. Any use of the computer or communications system for commercial, advertising, profit, or political purposes is prohibited.
5. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.
6. No use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.
7. Malicious or mischievous use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

8. Hate mail, chain letters, harassment, profanity, obscenity, racist and other antisocial behaviors are prohibited on the network.
9. Use of the network to access or process pornographic material, inappropriate text files (as determined by the system administrator or building administrator), or a file dangerous to the integrity of the network is prohibited.
10. Use of the network for any unlawful purpose is prohibited.
11. Playing games is prohibited unless specifically authorized by a teacher for instructional purposes.
12. Establishing network or Internet connections to live communications, including voice and/or video (relay chat) is prohibited unless specifically authorized by a teacher and a system administrator.
13. Sending offensive email (racist, pornographic, or otherwise inappropriate).
14. Harassment, intimidation, threatening, or engaging in any illegal activity.
15. Sending proprietary or confidential information to any unauthorized person.
16. Allowing other users access to your password or account.
17. Make changes to the operating system or networking settings.
18. Open up devices for repairs, etc.
19. Use of gambling, pornographic, or on-line actions sites/programs.
20. Tampering with any communications devices, i.e.; computers, phones, etc.
21. Changing of wiring, connections, or placement of computer resources is prohibited.
22. Use of school resources for any cheating or academic dishonesty.
23. Use of any hacking, cracking, password cracking, scanners, or any other hacking or network discovery tools.
24. Attempting to circumvent any security.
25. Starting any denial of services attacks.
26. Any unauthorized access to include wireless devices or any other communication devices.
27. Use of email systems or accounts other than those approved by the CIC staff and Superintendent.
28. Attempts to use the district's system for: Unauthorized solicitation of funds; distribution of chain letters; unauthorized sale or purchase of merchandise and services; collection of signatures; membership drives; transmission of any materials regarding political campaigns.
29. Saving inappropriate files to any part of the system, including but not limited to: Music files, movies, video games of all types, including ROMs and emulators, offensive images or files, programs which can be used for malicious purposes, any files for which you do not have a legal license, any file which is not needed for school purposes or a class assignment.

Disclaimer

1. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 *et seq*.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
2. The School Department will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained is at your own risk.

3. The School Department makes no warranties (expressed or implied) with respect to:
    - The content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information;
    - Any cost, liability or damages caused by the way the user chooses to use his or her access to the network.

Guest Access to the Network

1. Users must utilize the district's wired and wireless networks for access to the Internet in school district facilities using school district equipment. Guest users must utilize the district's wireless network BYOD to gain access to the Internet in school district facilities.
2. No other method or means of Internet access (i.e. USB modem, MiFi router, personal Internet access, open WiFi networks, etc.) is permitted while simultaneously connected to a district network or while using a district technology resource.

Content Filtering

1. The Rochester School District uses software designed to block access to certain sites and filter content as required by the Children's Internet Protection Act, 47 U.S.C. §254 (CIPA).
2. Upon request by staff, the Computer Department, under the director of the Superintendent, shall review and may authorize the disabling of Internet blocking/filtering software to enable access to specific educational related material that is blocked through technology protection measures, in accordance with applicable law and safe networking practices to protect the network.
3. Congress enacted the Children's Online Privacy Protection Act, 15 U.S.C. §6501, et seq. (COPPA) in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012 that became effective on July 1, 2013.
4. Each staff member has a firewall bypass account based on their position. These accounts shall not be shared with students or guest and will be supervised by staff members at all times.

The School Department reserves the right to change its policies and rules at any time.

Adopted:	January 14, 1997
Amended:	May 13, 2004
Board Review/Approved:	February 12, 2009
Amended:	September 10, 2015