ACCEPTABLE USE OF DISTRICT NETWORK

OBJECTIVES

This policy sets forth the standards and expectations governing use of the District's Network by all Rochester City School District ("District") Board members, employees, students, consultants, partners, and guests. The policy is intended to promote the ethical, legal, and school-related use of the District Network. All electronic devices will be governed under this policy when such devices are attached to the District Network.

RESPONSIBILITY

The purpose of District-provided computer, wired and unwired networks, email and internet access is to facilitate communications in support of legitimate District work, research and education. In order to remain eligible as Users, such use must support the educational objectives and work responsibilities of the District. Access is a privilege, not a right and access entails responsibility.

DEFINITIONS

1. District Network: All of the District owned or licensed computers, wired and unwired networks, email and telephone, hardware, software, and related technologies, including all networks, wiring, and communications equipment.

2. Electronic Information: All e-mail, audio files, and electronic data, files, or other records stored on the District Network

3. Educational Purposes: Those actions directly promoting the educational, instructional, administrative, business, and support services missions of the District and related to any District instruction, project, job, work assignment, task, or function for which the User is responsible.

4. Inappropriate Materials: Text, graphic, pictorial, or auditory representations of items that that, taken as a whole and with respect to the interests of students, appeal to a prurient interest in nudity, sex, or excretion; materials which lack serious literary, artistic, political, or scientific value to students; materials that promote discrimination or harassment against others based on race, religion, gender, nationality, sexual orientation; materials intended to teach skills that would enable an individual to engage in illegal activities; or materials that violate the law or are inconsistent with Policies of the Board of Education, Superintendent Regulations or the educational mission of the District.

5. Internet Access: All methods used to connect to Internet servers and Users, and all methods for providing access regardless of funding or facilitating sources, including e-mail.

6. **Restricted Information** – Any data or information for which the person accessing it does not have an educational purpose. This also relates to information that could be considered public where such information does not support User responsibilities in a manner that is beneficial to the District and personnel.

7. Technology Protection Measure: An Internet filtering technology that is designed to limit access to selected portions of the Internet based on identified criteria. Its intended use in the District is to limit access to Inappropriate Material.

8. Unauthorized Equipment: Any device that is not approved by the Superintendent or designee to be connected to a District computer or District Network, including, but not limited to personal communication and organization devices such as wireless access points, smart phones, or cell phones; gaming devices; photographic equipment; and entertainment devices such as MP3 players or iPods™.

9. User: Any Board of Education member, District employee, student, consultant, partner, guest or other individual authorized to use the District Network.

PROCEDURE

1. Management of Electronic Data and Information Security

   Users may only access information and/or computer systems to which they are authorized and that they need for their assignments and responsibilities.

   a. Users are responsible for their own individual accounts.

      i.) Users are required to protect the security of their accounts by changing passwords as directed by the Information Management and Technology Department ("IM&T") and by keeping their passwords strictly confidential.

      ii.) Users are expressly prohibited from sharing accounts and passwords.

      iii.) Violations that can be traced to an individual account name may be treated as the responsibility of the account owner.

b. IM&T shall develop and implement protocols in order that computers may be locked automatically when Users are away from their computers for a predetermined period of time. Users are required to log off before allowing others to use their computer.

It is the responsibility of every User to be aware of and follow all applicable security procedures in accordance with this Regulation.

c. Users must secure their electronic data. Sensitive files must be saved to a secure location such as an individual's network folder/directory or a removable disk that is then secured in a locked file cabinet.

d. Users should make backup copies of critical files stored on their computers and ensure the copies are stored in a secure place.

e. District Data and Information - Employees will only access information that; is necessary to perform their District duties consistent with the purpose intended; is consistent with the Code of Conduct; and does not qualify as **Restricted Information**.

2. Physical Security

Computer systems equipment must be located and maintained in a secure physical environment. Users are responsible for cooperating with the following physical security provisions for computers and related technology.

a. When staff members are not present to supervise the area, all areas (including permanent or temporary storage) housing valuable computer equipment must be secured.

b. Computer or related equipment, excluding laptops issued to individuals, may not be relocated or removed from District property without coordination through the Help Desk. Any computers or related equipment can only be moved from one location to another under the supervision of the District Computer Technician assigned to that building.

c. Users issued a laptop computer must sign a hand receipt when taking possession of the computer. The laptop must be returned to the IM&T Computer Services Liaison (located at Central Office) or School Technician prior to the User leaving the District or transferring to another school or office.

d. The Help Desk will maintain a database of all computers, computer equipment and cellular telephones signed out under a hand receipt. It is

the responsibility of the individual taking possession of the equipment and signing the hand receipt to notify the Help Desk that they have returned the equipment in order that their name may be removed from the database as a User in possession of the equipment.

e. District staff should report lost and/or stolen equipment by:

i.) Notifying the Police and filing a police report of stolen equipment.

(a.) Obtaining a copy of the Police Report and send one copy to:

(i.) The Director of Office of Safety and Security; and

(ii.) Information Technology Officer of IM&T.

ii.) Completing a Lost, Stolen or Damaged Computer Equipment Report Form listing all missing items with their serial number, make, model number and estimated costs. Copies should then be given to the Director of Office of Safety and Security and the Information Technology Officer of IM&T.

3. Systems and Applications Security

a. Users shall not install software or hardware, or disable or modify security settings or measures (such as antivirus software) installed on any computer for any purpose without the permission of the Help Desk.

b. Users must not change the system settings without the permission of the Help Desk.

c. District software and applications may not be installed or copied to a non- District computer, except when authorized in writing by the Information Technology Officer.

4. Network Security

The District is not responsible for information found on networks outside of the District, including, for example, the Internet. The District does not have control over information residing on other systems or Internet sites to which there is access through the District. Some sites and systems outside of District may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

a. Users are responsible for ensuring that access to or importation of material on networks is for Educational Purposes.

b. Any material or information purposefully posted or linked from the District system or Internet site must be consistent with the District's educational or business purpose, as defined in this Regulation.

c. Users are responsible for abiding by all Federal and State laws, Board policies and Superintendent Regulations applicable to the computer system(s) they use, including those accessed over the Internet from District equipment.

d. Except as provided in subparagraph e. and f. below, equipment owned personally by District employees, partners, or consultants may not be connected to the District Network or directly to any District owned equipment.

e. Requests of contractors or consultants to connect their corporate laptops or desktop computers to the District's Network shall be considered and approved in writing on a case-by-case basis by the Information Technology Officer or designee.

f. Approved contractors must sign a Network Access Request Form.

g. The only remote access or Virtual Private Network ("VPN") approved for all Users is to District Web pages through the Internet and to the District e-mail system. Remote access to all other District computer systems is not permitted, except by express written authorization of the Information Technology Officer.

i.) VPN access is only granted to District employees using District owned Window's based computer systems equipment

ii.) Employees may request VPN access for contractors with significant business justification and may be approved on a case-by-case basis by the Information Technology Officer or designee. Approved contractors must sign a District's VPN Access Request Form.

5. Conduct and Use

a. Use of all computer facilities, the District Network, and other technology resources are intended for Educational Purposes and are subject to District review and may be logged and archived.

b. District e-mail is for District Educational Purposes only. All emails are subject to District review and will be logged and archived.

i.) IM&T will assign an official District e-mail address to all employees. It is to this official address to which the District will send e-mail communications to employees. This official e-mail address will be the listed in the Global Address Book for the District's Exchange e-mail system.

ii.) Communications over the e-mail system shall be professional and appropriate for the workplace.

iii.) Falsifying mail headers or routing information so as to obscure the origins of mail or mail routes is forbidden.

iv.) Altering the content of a message attributed to another is not permitted unless the changes are expressly stated in the communication.

v.) The District will not support having e-mail electronically redirected to another e-mail address (e.g., @aol.com, @hotmail.com, @yahoo.com, etc.).

c. Given that communications may be time-critical, Users are expected to check their official e-mail address on a frequent and consistent basis in order to stay current with District communications.

d. All Users are prohibited from engaging in any unlawful activities or any other activities which would in any way bring discredit to the District.

e. Although it is impossible to identify every inappropriate conduct and use of computer facilities, the following examples of computer and network use infractions are expressly prohibited:

i.) Tampering with any portion of the District Network or assisting others to cause tampering (e.g. any unauthorized alteration of operating systems, individual accounts, network-shared folder, software, networking facilities, and/or other programs) and/or equipment damage.

ii.) Decrypting passwords, unauthorized capturing of passwords by using hardware devices or software applications, and/or gaining unauthorized higher-level access or privileges or attempting to do so.

iii.) Interfering deliberately with other Users' network access or computer use.

iv.) Using, possessing or distributing language, pictures, or other material or taking actions that are libelous, slanderous, or that harass others.

v.) Using, possessing or distributing Inappropriate Materials.

vi.) Introducing codes such as viruses or worms that may cause harm or subvert the intended function of District computer systems.

vii.) Attaching Unauthorized Equipment to any District computer or District Network without authorization from the Superintendent or designee.

viii.) Circumventing Technology Protection Measures, also known as network security or filtering technology.

ix.) Reading, deleting, copying, forging, or modifying the e-mail of other Users or attempting to do so.

x.) Reading, deleting, copying, forwarding, printing, sharing, or modifying the data files of other Users without the express written authorization of the Superintendent or designee.

xi.) Permitting another to use one's personal District e-mail address, account, or password.

xii.) Permitting another to use one's personal District Network account, network folders, or password.

xiii.) Using commercial advertising, personal solicitations, chain letters, or non-educational games on District systems.

xiv.) Copying or transferring copyrighted materials and software without authorization.

xv.) Using District Networks to post personally identifiable, confidential or false information about students or staff without proper authorization.

xvi.) Using District Networks or computer systems for personal gain or any illegal or unauthorized activity.

xvii.) Promoting political or religious causes.

xviii.) Distributing confidential District or student data or information without authorization of the Superintendent or designee.

xiv.) Any activity intended to foster personal financial gain.

xxi.) Any illegal purpose or action.

f. All Users are prohibited from knowingly accessing or attempting to access Inappropriate Material. Student and staff use of the Internet will be monitored by a variety of methods including, but not limited to, technology and direct supervision.

i.) At the discretion of the IM&T Director or designee, IM&T will take measures to block or filter Internet Access as required by the Children's Internet Protection Act. As a minimum, the following categories of sites will be blocked:

(a.) Violence - This category refers to sites that contain visual representations of or invitations to participate in violent acts. This may include war, crime, pranks, hazing, etc. A violent act may be considered any activity that uses physical force designed to injure another living being.

(b.) Weapons/bombs - This category refers to any site promoting the use of weapons and/or bombs and the making of bombs. This does not include sites related to gun control or legitimate social issues.

(c.) Adult themes and content - This category refers to sites that are adult in nature and are not defined in other rating categories.

(d.) Pornography - This category covers anything relating to pornography, including mild depiction, soft pornography and hard-core pornography.

(e.) Phishing - Deceptive websites intended to trick end-users into revealing personal data such as credit card numbers, account usernames, passwords, social security numbers, etc. These websites pretend to be those of common, well-known sites such as banks and credit card companies.

(f.) Social networking/dating - Sites that offer free or paid services that promote interaction, dating or other networking through forums, chat, email or other methods.

(g.) Intolerance/extremism - This category refers to any site advocating militant activities or extremism. This includes groups with extreme political views and intolerance to individuals and/or groups based upon discriminating or racial distinctions.

(h.) Spyware/adware - Websites that are known to distribute or contain code that displays unwanted advertisements or gathers information about the user without the user's knowledge.

(i.) Anonymizer - This category refers to sites that allow the User to surf the net anonymously. It also refers to sites that allow the User to send anonymous emails. This also includes sites providing proxy bypass information or services.

(j.) Copyright infringement - This category refers to sites that offer media, software, MP3, DVD movies or any other copyrighted materials that are bootlegged or illegally available for purchase or download. This category is often blocked to protect iPrism owners from liability caused by

the download and installation of bootlegged software. Note that this category does not refer to sites that are specific to computer hacking.

(k.) Nudity - This category refers to sites that provide images or representations of nudity. They may be in an artistic or non-artistic form such as magazines, pictures, paintings, sculptures, etc. This category shall be assigned to those sites that display both partial and full nudity even though the images may not be pornographic in nature.

(l.) Malware - Websites that are known to contain harmful code that may modify a User's system without the User's knowledge.

(m.) Local Deny – These are websites that have been identified but do not fall into one of the categories identified above.

ii.) IM&T will periodically review a trend report and make adjustments to what is blocked or filtered as required.

(a.) All Users are prohibited from knowingly accessing or attempting to access portions of the Internet that do not promote the educational, instructional, administrative, business, or support services purposes of District or are not related to any instruction, project, job, work assignment, task, or function for which the User is responsible.

(b.) Any User of the District Network who identifies a portion of the Internet that contains Inappropriate Material that has not been filtered through the Technology Protection Measure should contact the Help Desk immediately.

(c.) A User of the District Network shall not use those resources for personal commercial purposes or for personal financial or other gain.

(i.) Incidental personal use of the District Network for other purposes is permitted at the discretion of the Superintendent or designee when the use:

(1.) does not unreasonably consume those resources

(2.) does not interfere with the performance of the User's job or other District responsibilities;

(3.) does not consume an unreasonable amount of the User's work time;

(4.) does not concern subjects inappropriate in a school or work environment (e.g. accessing pornographic web sites);

(5.) is not inconsistent with the District's mission of teaching children;

(6.) is otherwise in compliance with applicable law, Policies of the Board of Education and Regulations of the Superintendent and;

(7.) is not **Restricted Information**.

6. Access to Confidential and other Electronic Information

a. Personally identifiable information about students contained in e-mail communications or attachments thereto, including information contained in student education records, medical information, and information about disabilities must be in compliance with the Family Educational Rights and Privacy Act ("FERPA") and the Health Insurance Portability and Accountability Act ("HIPAA").

b. District Employees may access the District's Electronic Information provided the employee needs to access the contents in order to perform the responsibilities of the job. Access shall be limited to that information necessary to complete the job responsibilities.

c. For non-BOE personnel and staff; Supervisors and other District personnel may access the Electronic Information stored anywhere on the District Network in order to review, retain or delete any or all e-mail messages, computer files, or electronic data used by an employee at any time provided permission to access that information has been approved by the District's General Counsel or designee and the Auditor General.

d. For BOE Personnel and staff, Supervisory personnel may access the Electronic Information stored anywhere on the District Network in order to review, retain or delete any or all e-mail messages, computer files, or electronic data used by an employee at any time provided permission to access that information has been approved by the Auditor General.

e. All requests for access to **Restricted Information** and approvals must be documented. The request must include the reason for the request, period of information requested, and specify any additional parties that will receive the information. Attachment 1 must be used to document the request.

f. No-one shall access nor disclose District Information and/or **Restricted Information** including but not limited to, financial information, personal information, students, parents, employees, or business partners for which they have not been authorized.

g. The Office of Auditor General of the BOE shall have full and unrestricted access to all systems, documents, and information within the Rochester City School District.

Any violation of this policy by a User (except District students) may result in denial of access and discipline consistent with the applicable collective bargaining agreement or employment rules and regulations of the Board and Superintendent, and applicable law. Any violation of this policy by a District student may result in denial of access and discipline consistent with the Code of Conduct (Policy 1400) and applicable law.

Adopted June 22, 2011 pursuant to Resolution No. 2010-11: 907; amended February 28, 2014 pursuant to Resolution No. 2013-14: 513