

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R

Planning and funding for computer networking in the District shall be handled in accord with the District's policy and rules on technology.

Supervised Use

Teachers are encouraged to use the District network in researching material for classes, collaborating with colleagues, developing innovative approaches, or otherwise enhancing their background, skills and teaching. Teachers are encouraged to make use of the District network in their classes when the use of the network enhances the students' education, is appropriately supervised, and is consistent with District goals and objectives. School administrators shall monitor technology use in the curriculum to ensure its effectiveness and develop ideas for further in-service instruction of staff.

When possible, school libraries and media centers will provide networked computers for students and staff to use for research purposes. Library/Media center staff shall make every reasonable attempt to assist users in the operation of the network and to monitor the content of material being accessed. Academic assignments have priority over personal research.

Any staff member who becomes aware of student network use in violation of the District's acceptable use rules shall refer the incident to the system administrator for action, and may remove the student from the computer.

Personal Accounts

No student, staff, or Board member network account shall be activated until the individual has submitted a District request for network access contract and been notified of the District rules for acceptable use of the network. Upon receipt of the contract, the system administrator will provide account, password, and other log-on information and instruction, including an initial disk space allocation where appropriate.

System Integrity and Security

Computer file servers containing student records, employee records, or other sensitive administrative documents shall be maintained on an electronically secured network protected from unauthorized access by outside entities, including student users.

All users, particularly staff, shall be instructed in password security. Passwords in general should not be (solely) English words available in common electronic dictionaries,

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R-2

nor should they be based on information, which is readily associated with the user (addresses, phone number, favorite flower, etc.). The system administrator may require a user to change a password if it fails to meet these criteria, or may issue randomly generated passwords to all users. Staff passwords should be changed every three months.

No user in a District building should leave a computer that is logged on to the network unattended without locking the workstation, and all users should promptly report any suspected breach of security or data integrity to the system administrator.

District Web Page(s)

Guidelines for Construction of Grand Rapids Public Schools WWW pages:

Purpose: District web pages should promote a positive image of the District and its programs. Web pages should facilitate and enhance the communication and educational goals of the District in a timely and professional manner.

Responsibility: The District web master is responsible for overseeing the content and design of all District web pages. The building Principals and/or their designees are responsible for developing web pages and content for their buildings and programs. The building Principals and/or their designees are responsible for entering data and uploading web pages.

A District Web Site Committee with a membership selected by the Executive Director of Management Information Systems and the building Principal(s) is/are responsible for developing guidelines and acting in an advisory capacity regarding all aspects of web page design and content.

Guidelines: These guidelines have been developed to ensure consistent quality and appropriate content of Grand Rapids Public Schools' web pages.

1. District web pages will be posted only on the District's server providing Internet access to the District as negotiated by the Executive Director of Management Information Systems. No "personal" or private web pages representing the District shall be allowed. (Example: A school "club" or individual classroom that might wish to post a web page through a "private/personal" home page would be disallowed.) Any staff member or students violating this rule shall be subject to disciplinary action under the student code of conduct or applicable collective bargaining agreements.

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R-3

2. The home page of each school and/or school program will present a consistent appearance. Contents, menus, background colors, heading styles, fonts, point sizes, buttons, icons, page sizes, and other graphic, and design elements should create unity within the array of the District's building and program pages.
3. Web pages will strive for high standards of professionalism with current and accurate information; correct grammar and spelling; and with no inappropriate reference to; race, gender, religion, politics, alcohol, drugs, firearms, or sex.
4. District web pages shall be free of all advertising and/or promotion of causes inappropriate to a public school educational setting.
5. No copyrighted text, graphics, or sound files will be used on District web pages without the express consent of the originator. It must be assumed that everything is copyrighted unless otherwise stated.
6. All updated and new pages must be proofread by someone other than the author/typist prior to uploading. Making sure the information is proofread is the responsibility of the person doing the uploading.
7. All links must be verified by someone other than the author/typist prior to uploading. This verification is the responsibility of the person doing the uploading.
8. Web pages linked from District web pages must have educational or school related value and be free of inappropriate references as stated in 3 and 4 above.
9. Permission of the parent(s)/guardian(s) must be on file prior to using a student's photo, name, and/or original work on the Internet (See attached form). Directory information of students (address, telephone number, and other personal information) will not be indicated on District web pages or used, in any form, on any District web page.
10. District pages that provide links to off-site web sites will include a disclaimer:
"The Grand Rapids Public Schools make every effort to provide a high quality web site with information and links that facilitate the accomplishment of our educational mission. Because of the unpredictable nature of the Internet however, we cannot be responsible for the content of pages not directly linked to this web site."

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R-4

**GRAND RAPIDS PUBLIC SCHOOLS
TECHNOLOGY USE AGREEMENT**

This form must be signed and returned to the school office before any school technology can be used.

I have read and hereby agree to comply with the Grand Rapids Public Schools Technology Use Policy. I further understand that any violation of the policy is unethical and may constitute a criminal offense. Should I commit any violation of the policy, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken.

USER FULL NAME:

First _____ Middle In. _____ Last _____

BUILDING _____ TODAY'S DATE _____

USER SIGNATURE _____

STUDENTS MUST COMPLETE THE FOLLOWING:

GRADE _____ ANTICIPATED YEAR OF GRADUATION _____

PARENT(S)/GUARDIAN(S) (Must be signed if applicant is under 18 years of age)

As parent(s)/guardian(s) of the student signing above, I have read and agree to the conditions set forth in the Grand Rapids Public Schools Technology Use Policy. I understand that this access is designed for educational purposes. I also recognize it is impossible for the Grand Rapids Public Schools to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. Further, I accept full responsibility for supervision if/when my child's use is not in a school setting. I hereby give permission for my child to access school technology and certify that the information contained on this form is correct.

I hereby _____ Give _____ Expressly withhold (Parent(s)/Guardian(s): Check one) permission for my child's photo, or any personal or Directory information to be published on District Web pages or the Internet. I _____ Do _____ Do Not (Parent(s)/Guardian(s) check one) give permission for my child's photo and name to be published on District Web pages or on the Internet as part of a "team" or other large group photo.

PARENT(S)/GUARDIAN(S) NAME (Please Print) _____

SIGNATURE _____ DATE _____

DISTRICT COORDINATOR AUTHORIZATION _____

Account Name: _____ Password: _____

06-29-09

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R-5

Limiting Access

School servers may incorporate blocking and filtering software. Sites may be blocked by the system administrator in response to a complaint by a student, staff member, Board member, or parent(s)/guardian(s) in accord with the District's procedures on controversial material.

E-mail sites, which deposit unsolicited, bulk, chain, or offensive messages on the District server, will be blocked. System administrators may also block e-mail following a complaint from any user. Time permitting; an effort will be made by the system administrator to notify the offending system operator of the violation and the District's desire not to be contacted in the future. The system administrator shall refer repeated violators, along with any case of solicitation for child abuse or other illegal act, to the Superintendent for action in concert with law enforcement authorities.

GRAND RAPIDS PUBLIC SCHOOL DISTRICT
RULES ON ACCEPTABLE USE OF COMPUTER NETWORK RESOURCES

Acceptable Use for Internet and District-Wide Area Computer Network

The District reserves the right to log Internet use and to monitor electronic mail space utilization by users. This means that there should be no expectation of privacy from the District's monitoring of student use of computer systems. The District will, at its discretion, review the sites and programs accessed by individual students, as well as the messages sent or received by individual students. Such monitoring will be conducted without any notice.

1. District Rights and Responsibilities

The Grand Rapids Public Schools (GRPS) is responsible for the management of the structure, hardware, and software that the District uses to allow access to information technologies for educational purposes. These include:

- a. Assigning and removing user accounts on the network(s);
- b. Maintenance and repair of equipment that comprises the network(s);
- c. Selection of software that the network will support;
- d. Defining the rights and responsibilities of users;
- e. Providing resources that support the mission of the District; and
- f. Providing training opportunities on the use, care, and application of information technology, including training in new technologies, software, and media as they are required and put into use in the District.

The District does not take responsibility for the content of resources accessed or located by users of technology. The District does not take responsibility for actions that do not support the purposes of the GRPS taken by users of technology.

The GRPS will periodically make determinations on whether specific uses of the Internet and/or District network are consistent with the Acceptable Use policy.

2. District Equipment

District equipment includes (but is not limited to) computers, drives, printers, scanners, networks, video and audio recorders, cameras, photocopiers, telephones, modems, and other related technological resources. Software includes (but is not limited to) computer software, print, and non-print resources. Networks include (but are not limited to) all voice, video, and data systems, including the District's internal network and the Internet.

3. Prohibited Student Activity

Students are prohibited from:

- a. Using technology available through Grand Rapids Public Schools for personal or private business, for product advertisement, or political lobbying or for incurring financial commitments on the Internet.
- b. Using technology to disrupt the activity of others, to harass or discriminate against others, to gain unauthorized access to computer systems or programs, or to plant any type of virus in any computer system or program.
- c. Using profanity, obscenity, discriminatory language, vulgarities, and other inappropriate language or graphics.
- d. Revealing any personal, confidential, or private information about other individuals, such as a home address, phone numbers, etc.
- e. Communicating that they are someone else, or that they are representing someone else or that they are representing the Grand Rapids Public Schools.
- f. Using someone else's account number or password or allowing someone else to use their account number or password.
- g. Using the system to obtain or disseminate pornography as it is defined by the Supreme Court.
- h. Ordering or making a commitment to pay for goods or services without proper authorization.
- i. Using technology to do anything unlawful, including violating any federal or state copyright or unfair trade laws.

- j. Conducting any activity that exposes the district to litigation or expenses.
 - k. Violating any libel or slander laws.
4. Student-Developed Subject Matter
- Definition: "Student Developed Subject Matter" means subject matter conceived or developed by the student during the student's use of GRPS systems, where such subject matter pertains or could pertain directly or indirectly to the then current educational activities of the GRPS. Whether subject matter falls within the scope of Student-Developed Subject Matter shall be independent of whether the student's contribution to the development is alone or in collaboration with others. Student-Developed Subject Matter shall include (but not be limited to) writings, designs, software, video, audio, and other materials and concepts which may be subject to proprietary rights protection. Disclosure and Assignment to the GRPS: The student shall promptly disclose to the GRPS all Student-Developed Subject Matter, and all Student-Developed Subject Matter shall become and remain the exclusive property of the GRPS. To the extent that any proprietary rights (including copyright rights) vest in the student as a result of the development of the Student-Developed Subject Matter, and to execute any documents considered necessary by the GRPS to perfect its proprietary rights therein.
- The GRPS shall pay all expenses relating to the perfection of such proprietary rights. The election of whether or not to file formal applications for proprietary rights protection for the Student-Developed Subject Matter, and the manner of preparation and prosecution of the same, shall be solely within the discretion of the GRPS.
5. Student Rights and Responsibilities
- Student users of District equipment have the right to:
- a. Use all authorized hardware and software, when available, for which they have received training to facilitate learning and enhance educational information exchange.
 - b. Access information from outside resources which facilitates learning and enhances educational information exchange.

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R-9

- c. Access direct networks and the Internet to retrieve information, facilitate learning, and enhance educational information exchange.
Student users of District equipment are responsible for:
 - a. Utilizing technology in the school only for facilitating learning and enhancing educational information exchange consistent with the educational mission of the district and the school.
 - b. Maintaining the privacy of passwords and are prohibited from publishing or discussing passwords.
 - c. Keeping all inappropriate materials, inappropriate text files, or files dangerous to the integrity of the school's network, equipment, and software from entering the school via the Internet or any other mechanism.
 - d. Keeping hardware and software from being removed from school premises without prior consent.
 - e. Maintaining the integrity of the e-mail system and making only those e-mail contacts which facilitate learning and enhance information exchange.
 - f. Keeping all food and drink away from computers, printers, etc.
 - g. Adhering to all copyright guidelines and avoiding plagiarism.
 - h. Adhering to the rules (including network etiquette) established for the use of hardware, software, labs, and networks in the school and through remote access.
6. Response to Violations
Response by the school and/or District to activities in violation of the prohibitions and/or student responsibilities outlined in this policy and rules/regulations will be in accordance with the GRPS Uniform Disciplinary Code.

Rules Accepted: June 29, 2009

BOARD MEMBER REQUEST FOR COMPUTER NETWORK ACCESS

The District provides access to our computer network to members of the Board of Education to promote and enhance the work of the Board as a public body through communication, innovation, and sharing of resources. Access to the network is a privilege, not a right, and the Board, by majority vote, may restrict, suspend, or terminate any Board member user's account for proven violations of Board policy or these rules. In requesting an account for access to the network, the Board member agrees to the following terms and conditions.

1. Use of the network must be for the purpose of legitimate Board business consistent with the goals of the District and the laws of the State of Michigan.
2. All use of the network must be in accord with the District's rules on acceptable use of network resources, as updated from time to time by the District.
3. The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers, including but not limited to the loss of data, delays, non-deliveries, or service interruptions caused by its negligence or the users' errors or omissions.
4. The network provides access to third-party data and information over which the District has no control. Though the District may make efforts to block inappropriate material, users may be exposed to defamatory, inaccurate, or otherwise offensive material. Use of the network or any information obtained via the network is at the user's own risk. The District specifically denies any responsibility for the accuracy or content of information obtained through its services.
5. The user is solely responsible for all charges and fees, including outside telephone, printing, and merchandise purchases made through the network. The District is not a party to such transactions and shall not be liable for any costs or damages, whether direct or indirect, arising out of network transactions by the user.

Section 4000 – Business Management

4510-R Computer Network (Cf. 4520)

4510-R-11

6. The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney’s fees, incurred by the District relating to or arising out of any breach of the terms of this request for network access.
7. The user acknowledges that the District's computer network belongs solely to the District and that any files, records, electronic mail, or other communication may be examined, edited, or deleted by the District at any time, in accord with District policy or regulations. In general, electronic mail in personal accounts will not be inspected without the consent of the sender or a recipient, except as necessary to investigate a complaint, or respond to a Freedom of Information Act request.
8. The User acknowledges that the school district may collect and store Personally Identifiable Information (PII).
9. The user acknowledges and understands that correspondence sent or received over the District's network may be subject to retrieval under the State of Michigan Freedom of Information Act, MCL 15.231 - 246.

I, as a member of the Board of Education, understand and agree to abide by the terms of this request for network access, and the District rules for acceptable use of network resources. I further understand that should I commit any violation, my access privileges may be revoked by majority vote of the Board. In consideration for using the District's network connection and having access to public networks, I hereby release the school District and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use, the network.

Board Member's Signature

Date

06/29/09