Grass Lake Community Schools
Technology Use and Safety
Administrative Guidelines

POLICY

The School Board (hereinafter referred to as the Board) of Grass Lake Community Schools, (hereinafter referred to as the District) recognizes that as technologies affect the manner in which information may be accessed, communicated and transferred by members of society, those changes may also alter instruction and student learning. Telecommunications, electronic information services and networked services significantly alter the information landscape by opening schools, classrooms and library media centers to a broader array of resources. The Board generally supports access by students to rich information resources, along with the development by staff of appropriate skills to analyze and evaluate such resources.

Telecommunications, including video, audio and text services, because they may be connected to any publicly available source in the world, will open classrooms to electronic information resources which may not have been specifically chosen or previewed for use by students of various ages.

In making decisions regarding student access to telecommunications and networked information resources, the Board considers its own stated educational mission, goals and objectives. This policy requires that all instructional and library media materials support and enrich the curriculum, while taking into account the varied instructional needs, learning styles, abilities and developmental levels of the students.

It is the policy of the Board to maintain an education and work environment which is free from all forms of bullying and unlawful harassment. Bullying or other aggressive behavior toward a student by electronic means (cyberbullying) is strictly prohibited. For details, definitions and possible disciplinary actions see sections 5517 and 5517.01 of the Grass Lake Community Schools Bylaws and Policies document at http://www.neola.com/grasslake-mi.

Additionally, it is the policy of the Board that the District will maintain full compliance with the Children's Internet Protection Act (CIPA) and the Family Educational Rights and Privacy Act (FERPA). CIPA is a federal law enacted by Congress in 2000 to address concerns about access to offensive (or threatening) content over the Internet on any school or library computers. A more detailed description of CIPA is available at http://www.fcc.gov/consumerfacts/cipa . FERPA is a federal law enacted in 1974 that protects the privacy of student educational records and "directory" information. A more detailed description of FERPA is available at http://www.ed.gov/policy/gen/guid/ferpa .

SCOPE

The Technology Use and Safety Administrative Guidelines delineate the procedures in place to ensure that the District complies with all Federal, State and Local statutes regarding:

1. Hardware
2. Software
3. Network/Internet
4. Electronic Mail
5. Security
6. Discipline
7. Copyright

The Administrative guidelines also explain the Technology Protection Measures used to block or filter Internet access to pictures and content that:

1. Are obscene
2. Contain child pornography
3. Are harmful or threatening to minors
4. The district determines is inappropriate for minors

The District currently employs an Internet content filtering system from M86 Security. While the system is used in collaboration with nearby districts and housed at the Jackson County ISD, it still allows local control of student access to Internet sites.

The Technology Use and Safety Administrative Guidelines also outline the specific responsibilities of the District, Staff and Students.

IMPLEMENTATION

The Board authorizes the Office of the Superintendent to prepare appropriate Administrative Guidelines for implementing this policy and for reviewing and evaluating its effect on instruction and student achievement. The Office of the Superintendent is also authorized to revise the Administrative Guidelines to incorporate recent changes in Federal, State or Local statutes to ensure compliance. Both the Policy and the Guidelines shall be available for review by parents, guardians, students, staff, and other members of the community. Further, all provisions of both Policy and the Guidelines are subordinate to local, state and federal statute.

I. Foreword

Use of technology at Grass Lake Community Schools, hereinafter referred to as the District, is a privilege extended to students and staff to enhance learning and exchange information. Use must be consistent with the mission of the District, and where appropriate, must comply with the stated purposes and use policies of any other networks used.

Users are responsible for using technology only for facilitating learning and exchanging information consistent with the mission of the District. Users must not use District technology on behalf of outside organizations without administrative approval. District technology is a closed forum. Occasional authorized approval for non-school related purposes or on behalf of outside organizations does not give rise to a right to such use in the future and does not create a limited open forum.

Messages and documents are the property of the District, and the District has the right to supervise the use of such property. Users shall have no expectation of privacy when using District technology. The District also has the right to revoke the user's access privileges any time for any reason.

Unless otherwise specified, the following regulations shall apply equally to all students, employees, volunteers, and all other users of the District network. Employees, volunteers, and users outside the school community may have additional obligations or access privileges owing to the nature of their positions.

With the privileges of membership in the District technology community comes responsibility. Users need to familiarize themselves with these responsibilities. Failure to follow them will result in loss of network privileges and/or disciplinary action as outlined in the Code and respective Board of Education policies.

The District shall not be held responsible for any individual's inappropriate use of its technology in violation of the law.

Each user shall be held personally, civilly and criminally responsible for any violations of the law. Each user of technology shall read and sign the Acceptable Use Guidelines summary page before using District technology. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Use and Safety Policy.

A violation of the Technology Use and Safety Policy will be documented in a District Incident Report, and processed according to District procedures.

II. Hardware

A. User Privileges
Users have the privilege to use all hardware for which they are authorized and have received training. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Policy.

B. User Responsibilities
1. Users are responsible for using technology only for facilitating learning and exchanging information consistent with the mission of the District.
2. Users are responsible for properly using and caring for the hardware. Users are to seek assistance if necessary.
3. Users must not use the hardware on behalf of outside organizations without administrative approval.
4. Users must not use the hardware for illegal activity.
5. Users must not use the hardware to find obscene or pornographic material.
6. Users must not disrupt the operation of individuals or the technology through altering or abusing the hardware.
7. Student users must use the hardware under the supervision of a staff member or his/her authorized representative.
8. Users must follow all copyright guidelines as stated in Section VIII.
9. Users are responsible for any costs or fees or repair costs for damages as outlined in Section VII.
10. Any misuse of the hardware will result in disciplinary action as stated in Section VII, and may also result in legal action if appropriate.

C. District Responsibilities
1. The District does not warrant that the functions of the system will meet any specific requirements the user may have, or that it will be error-free, or that its operation will not be interrupted. The District will not be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or use time) sustained or incurred in connection with the use, operation, or inability to use the hardware.
2. The District does not warrant any system to be absolutely secure.
3. The primary purpose of the District hardware shall be in support of the academic program and shall take precedence over professional support, and general information.
4. The Superintendent or his/her designee will periodically make determinations on whether specific uses of the hardware are consistent with this policy. The District reserves the right to monitor use. Therefore, the District reserves the right to limit or deny access any time, for any reason.
5. District staff will demonstrate good faith efforts to supervise use of hardware under their charge.

III. Software

A. User Privileges

Users have the privilege to use all software for which they are authorized and have received training. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Policy.

B. User Responsibilities

1. Users are responsible for using software only for facilitating learning and exchanging information consistent with the mission of the District.
2. Users must not place unauthorized information, computer viruses, or harmful programs on or through the computer system in either public or private files or messages.
3. Users must not disrupt the operation of individuals or the technology through altering or abusing the software.
4. Student users must use the software under the supervision of a staff member or her/his authorized representative.
5. Users are responsible for properly using and caring for software.
6. Users are to seek assistance if necessary.
7. Users must not use software on behalf of outside organizations, without administrative approval.
8. Users must not use software for illegal activities.
9. Users must not use software to create or find obscene or pornographic material.
10. Users must follow all copyright guidelines as stated in Section VIII (this includes any illegally installed copyrighted software, or the transferring of files, shareware, or software from information services without permission of the facilitator.)
11. Users are responsible for managing personal files and deleting old files in a timely manner.
12. Users are responsible for any costs or fees or repair costs for damages to the software as outlined in Section VII.
13. Any misuse will result in disciplinary action as stated in Section VII, and may result in legal action if appropriate.

C. District Responsibilities

1. The District does not warrant that the functions of any District-authorized software will meet any specific requirements that the user may have, or that it will be error free, or that its operation will not be interrupted. The District will not be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or time) sustained or incurred in connection with the use, operation, or inability to use the District software.
2. The District does not warrant any system to be absolutely secure.
3. The primary purpose of the District software shall be in support of the academic program and shall take precedence over professional support, general information, and recreation.

4. The Superintendent or his/her designee will periodically decide whether specific uses of the software are consistent with this policy. Therefore, the District reserves the right to monitor use. The District reserves the right to limit or deny access any time for any reason.
5. District staff will demonstrate good faith efforts to supervise the use of software under their charge.

IV. Network/Internet

A. User Privileges

Users have the privilege to use all District network resources, both internal and external (such as Internet), for which they are authorized and have received training. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Policy.

B. User Responsibilities

1. Users are responsible for using the network only for facilitating learning and exchanging information consistent with the mission of the District.
2. The student user may only log on and use the network under the immediate supervision of a staff member or authorized representative and only with an appropriate user account
3. The student is responsible for the use of her/his account and/or access privilege. Any problems that arise from the use of a student's account are the responsibility of the account holder.
4. Users must use only their account ID. Use of an account by someone other than the registered account holder is forbidden.
5. Users must not intentionally seek information on, obtain copies of (misappropriating), or modify files or other data belonging to other users.
6. Users must not misrepresent others on the network, or represent others without being explicitly authorized to do so.
7. Users must not disrupt the operation of the network through altering or abusing the hardware or software on the network.
8. Users must not use the network for sexual harassment, hate mail, profanity, vulgar statements, discriminatory remarks, defamatory statements or other remarks that would constitute noncompliance with the District's policies dealing with sexual, racial, or other types of harassment.
9. Users must not access pornographic material, educationally unsuitable files or files dangerous to the integrity of the network.
10. Users must not place unauthorized information, computer viruses, or other harmful programs on or through the computer system in either public or private files or messages, or otherwise interfere with others' use of the network.
11. Use of the network is for school purposes. Personal use should be limited according to the Superintendent's Administrative Guidelines. Staff members are encouraged to keep personal records and personal business at home.
12. Users are responsible for managing their personal files and deleting old files in a timely manner.
13. Users may not use the network on behalf of outside organizations, without administrative approval.
14. Users must follow all copyright guidelines as stated in Section VIII. (This includes illegally installed copyrighted software, or the transferring of files, shareware, or software from information services and electronic bulletin boards without the permission of the facilitator.)

15. Users are responsible for any costs or fees for information services or repair costs for damages to the Network as outlined in Section VII.
16. Any misuse will result in disciplinary action as stated in Section VII, and may also result in legal action if appropriate.

C. District Responsibilities

1. The District operates a Technology Protection Measure that blocks or filters Internet access to pictures and content that:
    a. Are obscene
    b. Contain child pornography
    c. Are harmful to students
    d. The district determines is "inappropriate for students"
2. The District blocks students access to e-mail, chat rooms, and other forms of direct public-forum electronic communications (e.g. Instant Message services).
3. Where direct electronic communications between students are necessary for curriculum-related collaboration, such communications occur in a closed forum and are monitored by District staff.
4. The District prohibits unauthorized disclosure, use and dissemination of personal identification information regarding students using District technology.
5. The District prohibits computer hacking and other unlawful activities by students using District technology.
6. The District employs measures (such as supervision and monitoring) to restrict students' access to material harmful to students.
7. The District does not warrant that the functions of any District-authorized software will meet any specific requirements that the user may have, or that it will be error free, or that its operation will not be interrupted. The District will not be liable for any direct or indirect, incidental or consequential damages (including lost data, information, or time) sustained or incurred in connection with the use, operation, or inability to use the network.
8. The District does not warrant any system to be absolutely secure.
9. The primary purpose of the network shall be in support of the academic program and shall take precedence over professional support, general information, and recreation.
10. The District reserves all rights to material stored in files on the network and will remove any material that the District, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable, educationally unsuitable or materially and substantially disruptive.
11. The Superintendent or his/her designee will periodically decide whether specific uses of the Network are consistent with this policy. The District reserves the right to log Internet use and monitor fileserver space utilization by users. Therefore, the District reserves the right to limit or deny access any time for any reason.
12. District staff will demonstrate good faith efforts to supervise the use of the network under their charge.
13. The use of District technology constitutes consent, under the Electronic Communications Privacy Act, on the part of all users to allow the District and its agents to intercept and access the e-mail and network/internet history information of each individual user.

V. Electronic Mail

A. User Privileges

Users have the conditional privilege to use electronic mail for which they are authorized and have received training. Staff may send e-mail to any member on the network or the Internet; prior approval is not required. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Policy.

B. User Responsibilities

1. Users are responsible for using e-mail only for facilitating learning and exchanging information consistent with the mission of the District.
2. Users must use only their account ID. Use of an account by someone other than the registered account holder is forbidden.
3. Users must not intentionally seek information on, obtain copies of (misappropriating), or modify files or other data belonging to other users.
4. Users must not misrepresent others on e-mail, or represent others without being explicitly authorized to do so.
5. Users must not disrupt the operation of the e-mail through altering or abusing the hardware or software on e-mail.
6. Users must not use e-mail for sexual harassment, hate mail, profanity, vulgar statements, discriminatory remarks, defamatory statements or other remarks that would constitute noncompliance with the Districts' policies dealing with sexual, racial, or other types of harassment.
7. Users must not place unauthorized information, computer viruses, or other harmful programs on or through the computer via e-mail.
8. Use of the e-mail is for school purposes. Personal use should be limited according to the Superintendent's Administrative Guidelines. Staff members are encouraged to keep personal records and personal business at home.
9. Users must follow all copyright guidelines as stated in Section VIII. (This includes illegally installed copyrighted software, or the transferring of files, shareware, or software from information services and electronic bulletin boards without the permission of the facilitator.)
10. Users are responsible for any costs or fees for information services or repair costs for damages to the e-mail system as outlined in Section VII.
11. Any misuse of e-mail will result in disciplinary action as stated in Section VII, and may also result in legal action if appropriate.
12. Users may not use e-mail on behalf of outside organizations, without administrative approval.

C. District Responsibilities

1. The District blocks students access to e-mail, chat rooms, and other forms of direct public-forum electronic communications (e.g. Instant Message services).
2. Where direct electronic communications between students are necessary for curriculum related collaboration, such communications occur in a closed forum and are monitored by District staff.
3. The District does not warrant that the functions of the system will meet any specific requirements that the user may have, or that it will be error free, or that its operation will not be interrupted. The District will not be liable for any direct or indirect, incidental or consequential damages (including lost data, information, or time) sustained or incurred in connection with the use, operation, or inability to use the system.
4. The District does not warrant any system to be absolutely secure.
5. The primary purpose of the District electronic mail system shall be in support of the academic program and shall take precedence over professional support, general information, and recreation.
6. The District reserves all rights to material stored in files on its e-mail system that are generally accessible to others and will remove any material that the District, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable, educationally unsuitable or materially and substantially disruptive.
7. The Superintendent or his/her designee will periodically decide whether specific uses of e-mail are consistent with this policy. The District reserves the right to log e-mail use and monitor fileserver space utilization by users. Therefore, the District reserves the right to limit or deny access any time for any reason.
8. District staff will demonstrate good faith efforts to supervise use of the Network by the students under their charge, as appropriate to the age level.
9. The use of District technology constitutes consent, under the Electronic Communications Privacy Act, on the part of all users to allow the District and its agents to intercept and access the e-mail and network/internet history information of each individual user.

VI. Security

A. User Privileges

1. Users may expect to use the technology free of harassment of any kind, either physical or electronic.
2. Staff members have the privilege to use technology resources consistent with professional development needs.
3. Users have the privilege to use all authorized technology for which they have received training. Each person using the technology must complete the Technology Acceptable Use Summary form. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Policy.

B. User Responsibilities

1. Users experiencing harassment must report the problem immediately to the designated staff member.
2. Users identifying a security problem must notify the technology facilitator in charge. The problem is not to be shown to anyone.
3. Users are responsible for using technology only for facilitating learning and exchanging information consistent with the mission of the District.
4. Any relocation, removal, or modification of the technology equipment must have the permission of the facilitator.
5. Users must use only the accounts and account numbers assigned to them. They are responsible for the use of those accounts and access privileges. They are not to share accounts or leave accounts unattended. They are not to publish, share, or discuss passwords.
6. Users must use real names. Anonymity and pseudonyms are not allowed.
7. Users will not abuse the rights and property of others by intentionally seeking information on, or modifying, the files of others; nor will users place unauthorized information, computer programs or viruses in either the public or private files of others or the Network.
8. Users must comply with the Districts' policies dealing with sexual, racial, or other types of harassment. Users will not divulge personal data to which they have access without explicit authorization to do so.
9. Users must not access pornographic material, inappropriate text files, or files dangerous to the integrity of the network.
10. Users are responsible for any costs or fees for information services or repair costs for damages as outlined in Section VII.
11. Any misuse will result in disciplinary action as stated in Section VII.

C. District Responsibilities

1. The District does not warrant that the functions of the system will meet any specific requirements that the users may have, or that it will be error-free, or that its operation not be interrupted. The District will not be liable for any direct or indirect, incidental, or consequential damages (including lost data information, or use time) sustained or incurred.
2. The District does not warrant any system to be absolutely secure.
3. The primary purpose of the District technology shall be support of the academic program and shall take precedence over professional support, general information, and recreation.
4. The District reserves the right to review materials stored in files on the Network that are generally accessible to others and will remove any material that the District, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable, educationally unsuitable or materially and substantially disruptive.

5. The Superintendent or his/her designee will periodically decide whether specific uses of the technology are consistent with this policy. The District reserves the right to monitor use. The District reserves the right to limit or deny access any time, for any reason.
6. District staff will demonstrate good faith efforts to supervise technology under their charge.

VII. Discipline

Users violating the privileges outlined in the District Technology Use and Safety Policy will be subject to disciplinary action. Violations include but are not limited to:

1. Intentionally seeking information on, obtaining copies of (misappropriating), or modifying files, other data, passwords belonging to other users.
2. Misrepresenting others on the Network, or representing others without being explicitly authorized to do so.
3. Disrupting the operation of the Network through alteration or abuse of the hardware or software.
4. Malicious use of the Network through hate mail, profanity, vulgar statements, discriminatory remarks or other noncompliance with the Districts' policies dealing with sexual, racial, or other types of harassment.
5. The placing of unauthorized information, computer viruses, or harmful programs on or through the computer system in either public or private files or messages, or otherwise interfering with others' use of the Network.
6. Illegal installation of copyrighted software.
7. Unauthorized downloading, copying (transmission), or use of licensed or copyrighted software.
8. Transferring files, shareware, or software from information services and electronic bulletin boards without permission.
9. Using a computer I.D. or account, other than his/her own.
10. Allowing anyone to use another's account.
11. Access to the Network and Internet without permission.

Student users violating any of the above regulations will be subject to a range of consequences including, but not limited to, losing computer privileges, suspensions from school and expulsion, depending on the severity of the infraction. All offenses will be recorded in the student's permanent file.

Additional Action:
All users violating the above code may face additional disciplinary action deemed appropriate in keeping with the disciplinary policies and guidelines of the school.

Cases that involve violations of state, local or federal laws could result in criminal prosecution and/or requirement of financial restitution.

VIII. Copyright

A. User Privileges

Users have the privilege to use all hardware or software for which they are authorized and have received training. Use of District technology shall constitute agreement and consent to abide by the terms set forth in the Technology Policy.

B. User Responsibilities

1. The use of copyrighted software without authorization is prohibited. Users are further prohibited from installing any copyrighted software or materials on the District hardware without proper authorization.
2. Users are prohibited from copying copyrighted materials from software, networks or other electronically accessible sites, without proper authorization.
3. Users must follow these copyright guidelines in the use of hardware and software, and in the transmission or copying of any text or files. Plagiarism rules apply to the electronic medium and to print materials.
4. Users must assume that NOTHING ON THE INTERNET IS IN THE PUBLIC DOMAIN unless the author specifically puts notice there, or if the information is used after the expiration of the copyright. If any use is found to be illegal, the user is responsible.

C. District Responsibilities

1. The Superintendent or his/her designee will periodically decide whether specific uses of the technology are consistent with respect to copyright law. The District reserves the right to monitor use. The District reserves the right to limit or deny access any time, for any reason.
2. The Superintendent or his/her designee reserves the right to review materials stored in files on the network and will remove any material that the District, at its sole discretion, believes to be a violation of copyright. The District reserves the right to remove a user account to prevent any further unauthorized activity.
3. The Superintendent or his/her designee will make reasonable steps to inform all staff and students of the District adherence to copyright policy and procedure.