Employee/Student Computer Use Agreement

GENERAL
Computer Use and Internet Access is a service provided for students and staff members by Madison School District 321. Use of this district's computer networking services must be directly related to an educational goal and consistent with the instructional objectives of this district. The district reserves the right to monitor **all** activity on the computer network service.

Building Principals and the System Administrators of the computer network service are district employees who are responsible for monitoring use of the system (computer network service and related equipment) by staff and students.

The computer network services provided by this district may not always meet student or staff requirements or be uninterrupted or error-free. It is provided on an "as-is, as available" basis. No warranties are made or given with respect to any service, information, or software contained therein.

PRIVILEGES AND RESPONSIBILITIES
The use of this district's computer network service for staff and students is a **privilege**, not a right. Permission from parents/guardians is required before students may access the computer network service. All users must sign an Acceptable Use Agreement before access is permitted. Upon acceptance for use of the computer network service, students and staff will be given a user ID (name) and password.

Student and staff freedom of speech and access to information will be honored; however, this district reserves the right to monitor and review all electronic transmissions and activities. User access may be denied, revoked, or suspended at any time because of inappropriate use. Further disciplinary action may also occur.

INFORMATION CONTENT
This district provides students and staff access to other computer systems through the Internet and users may encounter information that is controversial or potentially harmful. Because the information and sources of information on such computer network services is continually changing, it is impossible for the district to monitor all the content. Some computer systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal materials. This district does not condone the use of such materials and does not knowingly permit use of such materials in the school environment. Students or staff bringing such materials into the school environment will be dealt with according to the discipline policies of the individual schools and this district. Intentionally accessing or using such materials may result in termination of access to this district's computer network service capacities as well as in-school suspension, suspension from school or expulsion; or disciplinary actions for staff, including termination.

INTERNET SAFETY FOR STUDENTS
The district will take appropriate steps to protect all students from access, through the district's computers, to visual depictions that are obscene, pornographic, or are harmful to minors, by installing and utilizing specific technology that blocks or filters Internet access to such visual

depictions. The District will work to prevent unauthorized access and activities such as hacking, cyber-bullying, disclosures and use or dissemination of personal information on social networking sites.

The building principal or system administrator may authorize the disabling of the Internet block or filter system only for the purpose of enabling access for bona fide research or other lawful purpose. Disabling of the Internet block or filter system by any other staff member or student will result in disciplinary action.

ONLINE USE

All district policies and school rules pertaining to behavior and communications apply to online use. The use of this district's computer network services capabilities must be for educational purposes only and be consistent with this district's mission.

1. Users are not allowed to access the district's computer network services for any private or commercial purposes. Users are not allowed to attempt to sell or offer for sale any goods or services that could be construed as a commercial enterprise, unless pre-approved by the board or superintendent.
2. Illegal activity is prohibited and may result in referral to law enforcement.
    a. Sending, receiving, or accessing obscene or pornographic material is prohibited.
    b. Sending, receiving, or accessing harassing, threatening, or objectionable material is prohibited.
3. Using programs to infiltrate a computing system and/or damage the software components is prohibited.
4. Students and staff will use the computer network service resources efficiently to minimize interference with others.
5. Users are responsible for making back-up copies as needed.
6. Users will not transmit materials, information, or software in violation of any local, state, or federal law.
7. Attempts to log in to the system using another user's account will result in termination of the offending user's account.

ONLINE CONDUCT

All users are required to abide by the generally accepted rules of computer network service etiquette. These include, but are not limited to, the following:

1. Users will not be abusive in their messages to others.
2. Users will not swear, use vulgarities or any other inappropriate language.
3. Users will not reveal personal information regarding others and should be cautious when revealing users' own personal information (home address, phone number, etc.).
4. The computer network service may not be used in such a way that use would disrupt the use of the computer network service by others.
5. All communications and information accessible via the computer network service should be assumed to be private property but open to district scrutiny, and review at any time.
6. Users will not submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material, nor encourage the use of controlled substances.

Any on-line conduct that is determined by the Principal or system administrator to constitute an inappropriate use of this district's computer network service or to improperly restrict or inhibit other users from using and enjoying this district's computer network service is strictly prohibited and may result in disciplinary action.

COPYRIGHTED MATERIAL

Copyrighted material will not be placed on any system connected to this district's computer network service without the author's written permission. The following will apply to copyrighted materials:

1. Only the owner(s) or persons specifically authorized may upload copyrighted material to the computer network service.
2. Users may download only that copyrighted material for which permission has been requested and granted, or that falls within the fair use exception to the copyright laws.
3. A user may redistribute a copyrighted program only with the express written permission of the owner or authorized person or as provided by the fair use exception.

ELECTRONIC MAIL

Electronic mail ("e-mail") is a private electronic message sent by or to a user in correspondence with another person having Internet mail access. The following provisions apply to e-mail:

1. Messages received by the computer network service are retained on the system until deleted by the recipient. A canceled computer network service account will not retain its e-mail. Users must remove old messages in a timely fashion. When an employee or student leaves the district, their account will be deleted. Please save any needed data or information before leaving the district.
2. The system administrators may remove e-mail messages if not attended to regularly by the users.
3. E-mail may be viewed by others. There is no guarantee of confidentiality.
4. The system administrators will not intentionally inspect the contents of e-mail sent by one user to an identified addressee, or disclose such contents to anyone other than the sender, or an intended recipient, without the consent of the sender or an intended recipient, unless required to do so by law or this district's policies, or to investigate complaints regarding e-mail which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
5. This district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any e-mail transmitted on this district's computer network service.

THIRD-PARTY SUPPLIED INFORMATION

Opinions, advice, services, and all other information expressed by students, staff, information providers, service providers, or other third-party personnel on the computer network service provided by this district are those of the individual and do not represent the position of this district.

DISK USE

The system administrators reserve the right to set quotas for disk use on the computer system. Users exceeding their quota will be required to delete files to return to compliance. Users may request that their disk quota be increased by submitting a request stating the need for the quota increase. In determining whether to grant the request, the designated administrator will review the space available and the reason for the request. The decision of the administrator regarding disk use is final and not appealable. A user who remains in non-compliance of disk space quotas after seven (7) days of notification will have his or her files removed by a system administrator.

SECURITY

Security on any computer system is a high priority. All district users will meet the following requirements:

1. If a user feels that he or she can identify a security problem on the computer network service, the user will notify a school/system administrator. The user will not demonstrate the problem to others.
2. Users may not let others use their account and password nor will they leave their account open or unattended.
3. Users will immediately notify a school/system administrator if their password is no longer secure, or if they have reason to believe that someone has obtained unauthorized access to their account.
4. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the computer network service.
5. No Computers or other network attached devices will be permitted that have not been set-up by and/or cleared through the system administrator.

DEFINITIONS

"Pornography or Obscenity" is defined as:
Any picture, image, graphic image file, or other visual depiction that: (1) taken as a whole, appeals to a prurient [i.e. erotic] interest; (2) depicts, describes or represents in a patently offensive way an actual or simulated sexual act or sexual contact or a lewd exhibition; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value. 18 U.S.C. § 1460.

"Child pornography" is defined as:
Any visual depiction . . . whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—(1) the product of such visual depiction involves the use or appearance of a minor engaging in sexually explicit conduct; (2) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct. 18 U.S.C. § 2246.

"Harmful to minors" is a visual depiction containing any picture, image, graphic image file, or other visual depiction that, taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and lacks serious literary, artistic, political, or scientific value to minors.

"Minor," for the purposes of this policy, is an individual who has not attained the age of 18.

VANDALISM

Vandalism will result in disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the computer network service, or any of the agencies or other computer network services that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.

STUDENT DISCIPLINE

Violation of this policy may result in the following disciplinary actions:

1. A student may lose computer privileges/network access. The duration of loss as determined by the Principal or school/system administrator. Students found to flagrantly or persistently violate this policy may lose all computer privileges/network service access for the school year, or for the duration of school attendance.
2. A student may be removed from class, suspended, or expelled from school if he or she engages in conduct on the computer network service that constitute flagrant or persistent violations of this policy or could be considered illegal, as defined by federal and/or state law. Students committing illegal acts may be referred to the local law enforcement agency.
3. Each student is responsible for any damage he or she may cause to this district's computers or to the computer network service. The student must pay all costs incurred in restoring the computer or the network service to its previous working order.
4. If a class requires the use of a computer and/or the computer network service, a student who has lost computer privileges under this policy will be allowed to participate under direct teacher supervision unless he or she has been removed from the class.

STAFF DISCIPLINE

1. A staff member may lose computer privileges and/or network access. The duration of loss will depend on the severity of the violation as determined by the building administrator.
2. A staff member may be disciplined, up to and including termination from employment, if he or she engages in conduct on the computer network service that constitutes flagrant or persistent violations of this policy or could be considered illegal, as defined by federal and/or state law. Staff members committing illegal acts may be referred to the law enforcement agency.

UPDATING USER ACCOUNT INFORMATION

The computer network service may occasionally require new registration and information from users to continue the service. Users must notify the designated administrator of any changes/deletions in user information (address, phone, name, etc.).

TERMINATION OF ACCOUNT

A user's access to, and use of, the computer network service may be terminated at any time by notifying a system administrator. An account that is inactive for more than thirty (30) days may be removed along with that user's files without notice given to the user.

An administrator reserves the right, at his or her sole discretion, to suspend or terminate users' access to and use of the computer network service upon any violation of this policy.

This district's administration, faculty and staff may request the system administrator to deny, revoke, or suspend specific user access.

Legal Reference: 17 USC Section 1001, et seq.
Children's internet Protection Act, Sections 1703 to 1721, USC Section

254(h)(1)

Idaho Code Sections 6-210, 18-2201 and 18-2202

Policy History:
Adopted on: January 15, 2009
Revised: March 19, 2013