District Appropriate Use Handbook

The Minidoka County School District #331 offers network computer access for students and staff. This handbook covers appropriate Internet and other network uses of school computers.

1. **Primarily for Educational Purposes:** The District provides students with an electronic network to support education and research and for the conduct of school business. Student personal use of computers that is consistent with the District's educational mission may be permitted during class when authorized by a student's teacher or appropriate administrator. Personal use of District computers and networks outside of class is permissible, but must comply with District policy. Use is a privilege, not a right. Students have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to access, monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and internet access. This includes **any and all information transmitted or received in connection with such usage, including** email and instant messages.
2. **Educational Purpose:**
    a. The District network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality personal research.
    b. The District network has not been established as a public access service or a public forum. The District has the right to place reasonable restrictions on the material you access or post through the system. You are also expected to follow the rules set forth in district and school building rules and the law in the use of the District network.
    c. The District network may not be used for commercial purposes. This means you may not offer, provide, or purchase products or services through the District network.
    d. The District network may not be used for political lobbying. But you may use the system to communicate with elected representatives and to express your opinion on political issues.
3. **Student Internet Access/District Email Account:**
    a. Elementary students will have Internet access only under direct supervision. Secondary students may obtain an account with the approval of their parent. This account may be revoked or suspended in accordance with the District regulations set forth in this handbook.
    b. Students and their parent must sign an Appropriate Use Agreement to be granted an individual account on the District network. This Agreement must be renewed on an annual basis.
4. **Unacceptable Uses of Network:**

The following are considered examples of unacceptable uses and constitute a violation of this policy. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

a. Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale, use, or purchase any substance the possession or use of which is prohibited by the District's student discipline policy, local, State, or federal law; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate local, State, or federal law; information pertaining to the manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials;

b. Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading another person's communications; sharing another person's pictures, private information, or messages without their permission; or otherwise using his or her access to the network or the internet;

c. Uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information. Users will immediately notify the school's system administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.

d. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying defined as using a computer, computer system, or computer network to convey a message in any format, including audio or video, text, graphics photographic, or any combination thereof, that is intended to harm another individual.

e. Uses that jeopardize the security of student access and of the computer network or other networks on the internet; uses that waste District resources including downloading very large files without permission from a teacher, unnecessary printing, and consuming excess file space on shared drives.

f. Uses that are commercial transactions, including commercial or private advertising. Students and other users may not sell or buy anything over the internet. Students and others should not give personal information to others, including credit card numbers and social security numbers.

g. The promotion of election or political campaigns, issues dealing with private or charitable organizations or foundations, ballot issues, or proselytizing in a way that presents such opinions as the view of the District.

h. Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, or materials that depict the sexual exploitation of minors.

i. Disclosing identifying personal information or arranging to meet persons met on the

internet or by electronic communications; sharing one's password with others or allowing them to use one's account.

j. Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee.

k. Posting or sending messages anonymously or using a name other than one's own.

l. Attempting to bypass internal or external security systems or controls using District equipment. Students and staff may only access the internet using the District network.

m. Plagiarism of material accessed online. Teachers will instruct students in appropriate research and citation practices.

n. Using the network while access privileges are revoked.

o. Students are prohibited from joining chat rooms or using school equipment or school systems for any such activity, unless it is a teacher-sponsored activity.

p. Students will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, etc.

q. Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes them feel uncomfortable.

r. Students will not attempt to gain unauthorized access to the District Network or to any other computer system through the District network. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

5. System Security

Students are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should they provide their password to another person. Doing so may result in possible suspension of access privileges.

Internet Safety

Each District computer with internet access shall have a filtering device that blocks access to visual depictions that are obscene, pornographic, harmful, or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The District will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or other material that is inappropriate and/or harmful to minors. The Superintendent or designee shall enforce the use of such filtering devices.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex,

or excretion; or

2. 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;
3. And, taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The term "harmful to minors" is also defined in Section 18-1514(6), Idaho Code as:

The quality of any material or of any performance of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:

1. Appeals to the prurient interest of minors as judged by the average person, applying contemporary community standards; and
2. Depicts or describes representations or descriptions of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse which are patently offensive to prevailing standards in the adult community with respect to what is suitable material for minors and includes, but is not limited to, patently offensive representations or descriptions of:
    a. Intimate sexual acts, normal or perverted, actual or simulated; or
    b. Masturbation, excretory functions, or lewd exhibits of the genitals or genital area. Nothing herein contained is intended to include or proscribe any matter which, when considered as a whole, and in context in which it is used, possesses serious literary, artistic, political, or scientific value for minors, according to prevailing standards in the adult community, with respect to what is suitable for minors.
    c. The quality of any material or of any performance, or of any description or representation, in whatever form, which, as a whole, has the dominant effect of substantially arousing sexual desires in persons under the age of 18 years.

Internet Filtering

Filtering is only one of a number of techniques used to manage student's access to the internet and encourage acceptable usage. It is not viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Anything that falls under at least one of the categories below shall be blocked and filtered. This list will be updated/modified as required.

1. Nudity/ pornography: Prevailing U.S. standards for nudity, provocative semi-nudity, sites which contain pornography or links to pornographic sites;
2. Sexuality: Sites which contain material of a mature level, images or descriptions of sexual aids, descriptions of sexual acts or techniques, sites which contain inappropriate personal ads;
3. Violence: Sites which promote violence, images or description of graphically violent acts, graphic autopsy or crime-scene images;
4. Crime: Information on performing criminal acts (e.g., drug or bomb making, computer hacking), illegal file archives (e.g., software piracy);

5. Drug Use: Sites which promote the use of illegal drugs, material advocating the use of illegal drugs (e.g. marijuana, LSD) or abuse of any drug. Exception: material with valid-educational use;
6. Tastelessness: Images or descriptions of excretory acts (e.g., vomiting, urinating), graphic medical images outside of a medical context;
7. Language/Profanity: Passages/words too coarse to be softened by the word filter, profanity within images/sounds/multimedia files, adult humor;
8. Discrimination/Intolerance: Material advocating discrimination (e.g., racial or religious intolerance); sites which promote intolerance, hate, or discrimination;
9. Interactive Mail or Chat: Sites which contain or allow inappropriate email correspondence, sites which contain or allow inappropriate chat areas:
10. Inappropriate Banners: Advertisements containing inappropriate images or words;
11. Gambling: Sites which allow or promote online gambling;
12. Weapons: Sites which promote illegal weapons, sites which promote the use of illegal weapons;
13. Self-Harm: Sites containing content on self-harm including cutting, and sites that encourage anorexia, bulimia, etc.; and
14. Judgment Calls: Whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

Filtering should also be used in conjunction with educating students to be "Net-smart";

1. Using recognized internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
2. Using "Acceptable Use Agreements";
3. Using behavior management practices for which internet access privileges can be earned or lost; and
4. Appropriate supervision, either in person and/or electronically.

The system administrator and/or Internet Safety Coordinator and/or building principal shall monitor student internet access.

Inappropriate Language:

1. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
2. Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
3. Students will not post information that could cause damage or a danger of disruption.
4. Students will not engage in personal attacks, including prejudicial or discriminatory attacks.
5. Students will not harass another person. Harassment is persistently acting in a manner

that distresses or annoys another person. If you are told by a person to stop sending them messages, you must stop.

6. Students will not knowingly or recklessly post false or defamatory information about a person or organization.

Respect for Privacy:

1. Students will not repost a message that was sent to you privately without permission of the person who sent you the message.
2. Students will not post private information about another person.

Plagiarism and Copyright Infringement:

1. Students will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
2. Students will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be very confusing. If you have questions, ask a MCSD staff member.

Inappropriate Access to Material:

Students will not use the MCSD system to access material that may be interpreted as

1. Harmful to minors;
2. Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district;
3. A product or service not permitted to minors by law;
4. Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others;
5. A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
6. Defamatory, libelous, reckless or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense or otherwise violates any law, rule, regulation, Board policy and/or administrative regulation.
7. Students will not use the District network to access material that is profane or obscene (pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (hate literature). While the District network does provide filtering of Internet content it is still your responsibility to avoid accessing inappropriate sites that may not be blocked.

a. A special exception for accessing material generally considered inappropriate may be made if the purpose is to conduct research and access is approved by both your teacher and your parent.

b. To request access to a blocked Internet site or to report an inappropriate site, you must contact the school building Technology Coordinator.

8. If students mistakenly access inappropriate information, he/she should immediately disclose this access in the manner specified by his/her school. This may protect the student against a claim that he/she has intentionally violated this Policy.

Online Access on School Computers Internal Email:

1. The district shall provide email accounts for all secondary students.

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the internet without the permission of a parent or guardian and the student or, if the student is 18 or over, the permission of the student. Students should be aware that conduct on the District's computer or using the District's server may be subject to public disclosure depending upon the nature of the communication. Users should never give out private or confidential information about themselves or others on the internet, particularly credit card numbers and social security numbers. Staff members may approve exceptions in the case of applications for college or employment. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Student Use of Social Media

Students will be held accountable for the content of the communications that they post on social media websites and are responsible for complying with District policy. Students may not disrupt the learning atmosphere, educational programs, school activities, or the rights of others.

All requirements of this policy apply to use of social media through the District network or equipment or as part of a class assignment.

Internet Access Conduct Agreements

Each student and his or her parent(s)/legal guardian(s) will be required to sign and return to the school at the beginning of each school year the Student Appropriate Use Contract prior to having access to the District's computer system and/or internet service.

Warranties/Indemnification

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the internet. The District will not be responsible for any unauthorized charges or fees resulting from access to the internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the

internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event the school initiates an investigation of a user's use of his or her access to its computer network and the internet.

Violations

If any user violates this policy, the student's access to the District's internet system and computers will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action. The **[system administrator OR the Internet Safety Coordinator OR the building principal]** will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his or her decision being final. Actions which violate local, State, or federal law may be referred to the local law enforcement agency.

If the actions of the individual are also in violation of other District discipline policies, said student shall be subject to additional possible disciplinary action based upon these policies.

Internet Safety Coordinator

The Superintendent shall serve, or appoint someone to serve, as "Internet Safety Coordinator" with responsibility and authority for ensuring compliance with the requirements of federal law, State law, and this policy. The Internet Safety Coordinator shall develop and maintain administrative procedures to enforce the provisions of this policy and coordinate with the appropriate District personnel regarding the internet safety component of the District's curriculum. The Internet Safety Coordinator shall handle any complaints about the enforcement of this policy or refer them to other appropriate personnel depending on the nature of the complaint.

The Internet Safety Coordinator shall maintain documentation evidencing that instruction by school personnel on internet safety is occurring District wide.

Public Notification

The Internet Safety Coordinator shall inform the public via the main District webpage of the District's procedures regarding enforcement of this policy and make them available for review at the District office.

Submission to State Department of Education

This policy shall be filed with the State Superintendent of Public Instruction every five years after initial submission and subsequent to any edit to this policy thereafter.

Your Rights:

1. **Free Speech**
    a. Your right to free speech, as set forth in the MCSD Student Code of Conduct,applies also to your communication on the Internet. The District network is considered a limited forum, similar to the school newspaper, and therefore the MCSD may restrict your speech for valid educational reasons.
2. **Search and Seizure.**

a. You should expect only limited privacy in the contents of your personal files on the District network and records of your online activity. The situation is similar to the rights you have in the privacy of your locker.

b. Routine maintenance and monitoring of the District network may lead to discovery that you have violated this Policy, the school building's rules, or the law.

c. An individual search will be conducted if there is reasonable suspicion that you have violated this policy, the school building's rules, or the law. The investigation will be reasonable and related to the suspected violation.

d. Parents of students have the right at any time to request to see the contents of their child's e-mail.

3. Due Process

a. The District will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the NWCSD Network.

b. In the event there is a claim that you have violated this Policy or the school building's rules in your use of the NWCSD Network, you will be provided with notice and opportunity to be heard in the manner set forth in your school building's rules.

c. If the violation also involves a violation of other provisions of your school building's rules, it will be handled in a manner described in the NWCSD policies. Additional restrictions may be placed on your use of your Internet account.

Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District network will be error-free or without defect. MCSD will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. MCSD is not responsible for the accuracy or quality of the information obtained through or stored on the system. MCSD will not be responsible for financial obligations arising through the unauthorized use of the system. Your parents can be held financially responsible for any harm to the system as a result of intentional misuse.

Password Security

All users of the District network shall adhere to follow the password guidelines:

1. Passwords must be at least eight characters long and include at least one upper case letter, one lower case letter, one number, and one of the following symbols (*, &, ^, %, $, #, @, !, +, _).
2. Users shall keep their password private and not share it with anyone.
3. Passwords shall be changed regularly and at least annually.
4. Student passwords will be automatically changed at the beginning of each school year until their signed Acceptable Use Agreement is turned in.

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE: ~~**I.C. § 18-1514(6) Obscene Materials – Definitions**~~
~~**20 U.S.C. § 9134(f) Children's Internet Protection Act**~~
~~**20 U.S.C. § 7131 Internet Safety**~~
I.C. § 18-917A Student Harassment – Intimidation – Bullying
P.L. 110-385 Broadband Data Services Improvement Act
Children's Internet Protection Act (CIPA) 47 U.S.C. § 254(h)(5)(B)-(C), 254(l)
Internet Safety 20 U.S.C. § 6777
Children's Internet Protection Act Certifications Required 47 C.F.R. § 54.520(c)(1)(i)

AMENDED: June 19, 2017; August 19, 2019

CROSS REFERENCE: Policy 226.00 Idaho Digital Learning Academy IDLA Classes