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 as well as the care and use of electronic devices.

Primarily for Educational Purposes

The District provides students and staff with electronic services including but not limited to electronic devices, computers, tablets, internet, and the overall network of systems and applications to support education, research, and conducting School District business. 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. Use of District electronic services establishes no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic Services. 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 electronic services of the district This includes any and all information transmitted or received in connection with such usage, including email and instant messages. The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Educational Purpose

- Limited Purpose: The District network has been established for educational purposes, including classroom activities, career development, and limited personal research.
- Content Restrictions: The District has the right to analyze and set restrictions on the material accessed or posted.
- Commercial Use: The District network may not be used for commercial purposes.
- Political Activity: The District network may not be used for political lobbying.

User Internet Access/District Email Account

- The District's electronic services are owned and controlled by the District. The District provides email to aid in fulfilling their duties and responsibilities and as an education tool.
- Elementary students have Internet access only under supervision, while secondary students may obtain an account with parental approval.
- An Appropriate Use Agreement must be signed annually for individual electronic services and account access. Users under the age of 18 requires Parent or guardians signature accompanied with theirs.

- Email could be subject to public records requests and disclosures depending upon the subject matter of the contents of the email.
- The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an electronic email account is strictly prohibited
- All users 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.

Unacceptable Uses of Network

The following actions are considered unacceptable and violate this policy:

- 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
- Harm to Others: Engaging in defamation, unauthorized use of passwords, or sharing private information without consent.
- Inappropriate Content: Accessing gambling sites, downloading harmful programs, or engaging in harassment.
- Disruption: Activities that jeopardize network security or waste resources.
- Unauthorized Transactions: Selling or buying anything via the internet.
- Personal Information: Sharing personal contact information.
- Damaging or destruction of electronic services: Taking proper care of school-issued electronic devices, including no defacement (e.g., stickers, drawings) and following guidelines for their use. Any damage or inappropriate alteration will result in fines and include disciplinary action.
- Uses that jeopardize the security of the computer network or other electronic services of the district.
- Waste of District resources including downloading very large files without permission from a teacher, unnecessary printing, and consuming excess file space on shared drives.
- Uses that are commercial transactions, including commercial or private advertising. Students and other users may not sell or buy anything over the internet. No personal

information should be given to others, including credit card numbers and social security numbers.

- 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.
- Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, or materials that depict the sexual exploitation of minors.
- 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.
- Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee.
- Posting or sending messages anonymously or using a name other than one's own.
- 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.
- Plagiarism of material accessed online. Teachers will instruct students in appropriate research and citation practices.
- Using the network while access privileges are revoked.
- Students are prohibited from joining chat rooms or using school electronic services for any such activity, unless it is a teacher-sponsored activity.
- No posting personal contact information regarding anyone. Personal contact information includes address, telephone, school address, work address, etc.
- Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes them feel uncomfortable.
- No user will attempt to gain unauthorized access to the District Network or to any other electronic service of the District. 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".

Internet Safety and Filtering

- All District electronic services 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:
  - Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
  - 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, 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:
  - Appeals to the prurient interest of minors as judged by the average person, applying contemporary community standards; and
  - 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:
  - Intimate sexual acts, normal or perverted, actual or simulated; or
  - 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.
  - 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.

Inappropriate Language and Behavior

- All forms of inappropriate language, harassment, personal attacks are prohibited. This includes but is not limited to:
  - Plagiarism (from any source or other individuals)
  - Students will not electronically display, send, or post private information about another person.

- Users will not access inappropriate information containing:
  - All activity listed in "Internet Safety "and "Internet filtering"
  - A product or service not permitted to minors by law
  - Content causing substantial disruption to school

❖ 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 the appropriate parties i.e. teachers and parents or the Superintendent.

❖ To request access to a blocked Internet site or to report an inappropriate site, you must contact the IT department.

❖ Inappropriate information accessed accidentally should be immediately closed. This may protect the student against a claim stating intentional violations.

Online Access and Confidentiality

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.

Password Security

- All users of the District network shall adhere to follow the password guidelines:
  - Passwords must be at least Twelve characters long and include at least one upper case letter, one lower case letter, one number, and one 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.
  - K-5 Passwords will be provided by the District and utilize alternative guidelines.

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.

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, 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 [Director of Information Technology OR the Internet Safety Coordinator OR the superintendent] 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 and Responsibilities

Free Speech

- 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.

Search and Seizure

- 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 like the rights you have in the privacy of your locker.
- Routine maintenance and monitoring of the District network may lead to the discovery that you have violated this Policy, the school building's rules, or the law.
- 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.
- Parents of students have the right at any time to request to see the contents of their child's e-mail.

Due Process

- The District will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the MCSD Network.
- In the event there is a claim that you have violated this Policy or the school building's rules in your use of the MCSD Network, you will be provided with notice and opportunity to be heard in the manner set forth in your school building's rules. 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 MCSD 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.

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE:

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; November 16, 2019; August 17, 2020; December 18, 2023

CROSS REFERENCE: Policy 226.00 Idaho Digital Learning Academy IDLA Classes