## Policy 3270P1 – District-Provided Access to Electronic Information, Service, and Networks – Acceptable Use of Electronic Networks

Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behaviors by users. However, some specific examples are provided. **Failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Terms and Conditions

1. ~~**[OPTION 1:**~~ **Educational Purposes Only**~~]~~ All use of the District's electronic network must be either in support of education or research and in furtherance of the District's stated educational goals; or for a legitimate school business purpose. 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 and any and all information transmitted or received in connection with such usage, including email and other messages.

   ~~**[OPTION 2: 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 and any and all information transmitted or received in connection with such usage, including email and other messages.~~

2. Privileges: The use of the District's electronic networks is a privilege, not a right, and Inappropriate use of the District's electronic networks may result in cancellation of those privileges. The system administrator **(AND/OR building principal** ~~**AND/OR Internet Safety Coordinator)**~~ will make all decisions regarding whether or not a user has violated these procedures, and may deny,

revoke, or suspend access at any time. An appeal of such decisions may be made to the Superintendent within seven days. Their decision is final.

3. Unacceptable Uses: The user is responsible for their actions and activities involving the network. Some examples of unacceptable uses are the following:

    A. Using the network for any illegal activity, or to access websites encouraging illegal activity including violation of copyright or of contracts, or transmitting any material in violation of any U.S. or State law;
    B. Accessing sites which allow or promote online gambling;
    C. Accessing information pertaining to the manufacture of weapons or the promotion of illegal weapons;
    D. Downloading the TikTok app or visiting the TikTok website;
    E. Uses that cause harm to others or damage property;
    F. Unauthorized downloading, installation, or copying of software, regardless of whether it is copyrighted or checked for viruses;
    G. Downloading copyrighted material or trade secret information;
    H. Viewing, transmitting, or downloading pornographic materials, materials harmful to minors, or other sexually explicit materials;
    I. Using the network for private financial or commercial activities;
    J. Wastefully using resources, such as file space or a printer;
    K. Hacking, attempting to bypass security systems, or gaining unauthorized access to files, resources, or entities;
    L. Uploading a worm, virus, or other harmful form of programming and other uses the jeopardize the security of the network;
    M. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;
    N. Using another user’s account or password or some other user identifier that misleads message recipients into believing that someone other than you is communicating;
    O. Posting material authored or created by another person, or pictures of another person, or another person’s private information or messages without his or her consent;
    P. Posting anonymous messages or messages using a name other than one’s own;
    Q. Using the network for commercial or private advertising;
    R. Uses that are commercial transactions;
    S. Accessing, submitting, posting, publishing, sending, or displaying any inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material;
    T. Accessing sites which promote violence or depict or describe graphic violence. This includes promotion of self-harm;

U. Accessing sites which advocate discrimination or which promote intolerance.
V. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying;
W. Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation;
X. Using the network while access privileges are suspended or revoked;
Y. Promotion of political, personal, or religious causes in a way that presents such opinions as the view of the District;
Z. Disclosing identifying personal information or arranging to meet persons met on the internet or by electronic communications;
AA. ~~[OPTIONAL]~~ Students are prohibited from using personal e-mail unless authorized to do so by District staff. 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; and

4. Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

   A. Be polite. Do not become abusive in messages to others.
   B. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
   C. Do not reveal personal information (including the addresses or telephone numbers) of other students or staff.
   D. Recognize that District email is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
   E. Do not use the network in any way that would disrupt its use by other users.

5. Security: Network security is a high priority. If the user can identify a security problem with the District's electronic devices or services, the user must notify the system administrator, Internet Safety Coordinator, or building principal. The user shall not demonstrate the problem to other users. Users shall keep their account and passwords confidential. Users shall not use another individual's account. Attempts to log on to the internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

6. Telephone Charges: The District assumes no responsibility for any unauthorized charges or fees, including telephone charges.

7. Copyright Web Publishing Rules: Copyright law and District policy prohibit the republishing of text or graphics found on the internet or on District websites or file servers, without explicit written permission.

    A. For each republication on a website or file server of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the website address of the original source.

    B. Students engaged in producing website pages must provide library media specialists with email or hard copy permissions before the website pages are published. Evidence of the status of “public domain” documents must be provided.

    C. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material is not necessarily authorized to act as a source of permission.

    D. The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

    E. Student work may only be published if there is written permission from both the parent/guardian and the student.

    F. Violation of the copyright web publishing rules may result in denial of access to the network.

8. Use of Email

    A. The District’s email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid students in fulfilling their duties and responsibilities and as an education tool.

    B. Email could be subject to public records requests and disclosures depending upon the subject matter of the contents of the email.

    C. 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 email account is strictly prohibited.

D. Each person should use the same degree of care in drafting an electronic email message that would be put into a written memo or document. Nothing should be transmitted in an email that would be inappropriate in a letter or memorandum.

E. Email sent from a District account carry with them an identification of the user's internet domain. This domain name identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this District. Users will be held personally responsible for the content of any and all emails transmitted to external recipients.

F. Any message received from an unknown sender should treated with caution and handled as directed by the system administrator. Downloading any file attached to any electronic based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

G. Use of the District's email system constitutes consent to these regulations.

Internet Safety

1. Internet access is limited to only those "acceptable uses," detailed in these procedures.

2. Staff members shall supervise students while students are using District internet access at school, to ensure that the students abide by the Terms and Conditions for Internet Access contained in these procedures.

3. Each District computer with internet access shall be equipped with a filtering device that blocks materials that are obscene, pornographic, or harmful or inappropriate for students as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The filter may also block other materials students are prohibited from accessing by District policy or procedure. The Superintendent or designee shall enforce the use of such filtering devices. Students must use the District's filtered network for all online activities on school grounds or using District equipment. Such filter shall also block access to the TikTok website. Measures shall also be undertaken to prevent the downloading of TikTok onto any District device or via the District's electronic network.

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

Student Use of Social Media

Students will be held accountable for the content of the communications that they post on social media locations and are responsible for complying with District policy and procedures for content posted using a District computer, network, or software or when posted during school hours when the student is in attendance at school. Student posts on social media locations outside of school hours and school grounds using a personal computer, network, and software shall be private as long as they do not enter into the educational setting and interfere with the orderly operation of the school. Posts to social network sites using a District computer, network, or software may be subject to public records requests. Students may not disrupt the learning atmosphere, educational programs, school activities, or the rights of others.

All of the requirements and prohibitions in District policy and procedure apply to the use of social media on school grounds, through the District network or using District equipment, or as part of a class assignment.

**Legal References:**

| **Legal References** | **Description** |
|---|---|
| 20 USC § 7131 | Internet Safety |
| 20 USC § 9134(f) | State Plans - Internet Safety |
| IC § 18-1514(6) | Obscene Materials — Definitions |
| IC § 18-6726 | TikTok Use by State Employees on a State-Issued Device Prohibited |
| IC § 33-132 | Local School Boards — Internet Use Policy Required |
| IC § 33-2508 | Digital and Online Library Resources for K-12 Students |
| Idaho Executive Order | 2022-06 |
| **Cross References** | |
| **Code** | **Description** |
| 2335 | Digital Citizenship and Safety Education |
| 2395 | Idaho Digital Learning Academy Classes |
| 3085 | Sexual Harassment, Discrimination, and Retaliation Policy |
| 3085-P(1) | Sexual Harassment, Discrimination, and Retaliation Policy - Title IX Sexual Harassment Grievance Procedure, Requirements, and Definitions |
| 3085-F(1) | Sexual Harassment, Discrimination, and Retaliation Policy - Notice of Investigation & Allegation Template |
| 3085-F(2) | Sexual Harassment, Discrimination, and Retaliation Policy - Reporting Form for Students |
| 3260 | Bring Your Own Technology Program |

| | |
|---|---|
| 3260-F(1) | Bring Your Own Technology Program - Permission Form |
| 3265 | Student Owned Electronic Communication Devices |
| 3275 | District Provided Mobile Computing Devices (Alternatives) |
| 3275-F(1) | District Provided Mobile Computing Devices (Alternatives) - AGREEMENT |
| 3330 | Student Discipline |
| 5325 | Employee Use of Social Media Sites, Including Personal Sites |
| 8705 | Generative Artificial Intelligence |