**DE SMET SCHOOL DISTRICT 38-2**
**NETWORK ACCEPTABLE USE POLICY**

---

**Definitions:**

Any reference to "District" in this policy shall refer to the De Smet School District 38-2.
Any reference to "State" in this policy shall refer to South Dakota Bureau of Information and Telecommunications (BIT) or State of South Dakota K12 Data Center.
Any reference to "Network" in this policy shall include computers (including Chromebooks), tablets (including iPads), peripherals, Intranet or Internet access, servers, routers, switches, access points, along with any other District or State technology or resource.
Any reference to "User" in this policy shall refer to any student, District employee, or guest using the District's Network.
Any reference to "AUP" in this policy shall refer to this Acceptable Use Policy.

**District Information:**

The District's AUP has been created to minimize the risk of unauthorized access and other unlawful activities by users online, to minimize the risk of unauthorized disclosure of or access to sensitive information, to comply with the Children's Internet Protection Act (CIPA), to comply with the Family Educational Rights and Privacy Act (FERPA), and to comply with the Children's Online Privacy Protection Act (COPPA). The AUP applies even when District equipment or resources are used off of District property.

The District reserves the right to monitor users' online activities and to access, review, copy, store, or delete any electronic communication or file and disclose them to others as it deems necessary in accordance with FERPA. Users should have no expectation of privacy regarding their use of District Network, property, or files stored on or accessed via the District Network.

**Regulations:**
The use of the District Network is not transferable or extendible by users to people or groups outside of those enrolled in or employed by the District and terminates when a District student or employee is no longer enrolled in or employed by the District. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. **If a person violates this policy, privileges may be terminated, access to the school district technology resources may be denied, and the appropriate disciplinary action shall be applied.**

Users are required to follow this policy. Users are also required to sign an acknowledgment of understanding of this policy annually, when required by the District, or when accounts are established for a limited educational purpose. The term "educational purpose" includes classroom activities, continuing education, professional or career development, extra-curricular events coverage, and high-quality, educationally enriching personal research.

**End-user District Assigned Devices:**

All devices assigned to users (Employees, Students, or Guests) remain the property of the District and are subject to repossession or inspection at any time by or at the direction of an appropriate administrator.

**Unacceptable Uses of the District Computer Network or Internet:**

The District Network has been established as a means to enhance or transform the educational experience for students and employees as well as giving employees access to education, communication, and productivity resources. The Network has **NOT** been established as a public access service or a public forum. The District has the right to place reasonable restrictions on any material you access, post, or create using its Network.

Below are examples of inappropriate activity on the District network. However, the District reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for students, the District, its Network, employees, schools, or other users not limited to guests on the Network or (2) that expend District resources on content the District, in its sole discretion, determines lacks legitimate educational content or purpose, or (3) that are determined to be inappropriate by the District.

- Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, plagiarism or copyrighted materials.
- Criminal activities that can be punished under law including but not limited to: copyright infringement, plagiarism, libel, slander, defamation, fraud, and illegal gambling.
- Downloading programs or files or accessing content that can be hazardous to the network without permission of the Technology Coordinator.
- Soliciting, selling, or purchasing illegal items or substances.
- Users knowingly accessing or bringing prohibited materials into the school environment may be subject to suspension and/or the termination of their privileges and will be subject to discipline in accordance with the district's policy and applicable administrative regulations.
    - Prohibited Material may not be accessed at any time, for any purpose. The district designated the following types of materials as Prohibited: obscene materials, child pornography, material that appeals to a prurient or unhealthy interest in, or depicts or describes in a patently offensive way, violence, nudity, sex, death, or bodily functions, material that has been designated as for "adults" only, and material that promotes or advocates illegal activities.
- Causing harm to others or damage to their property; such as:
    - Using profane, abusive, or impolite language; threatening, intimidating, harassing, or making damaging or false statements about others, or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
    - Deleting, copying, modifying, or forgoing other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
    - Damaging computer equipment, files, data, or the Network in any way, including intentionally accessing, transmitting, or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
    - Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws.
- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
    - Impersonation;
    - Forgery;
    - The use of others' account passwords or identifiers without prior consent;
    - Or the interference of others to access any Network account assigned to them.
- Circumventing District or State firewalls or filters using a Virtual Private Network (VPN), a Proxy Server, or any other means.
- Attempting to or accessing a local or Network administrator account without prior approval of the Technology Coordinator.
- Using the Network for Commercial purposes:

    - Using the Internet for personal financial gain, personal advertising, and promotion; or
    - Conducting for-profit business activities or engaging in non-District related fundraising or public relations activities such as solicitation for religious purposes or lobbying for personal political purposes.
- Using Social Media:
    - Users may not use social media sites to publish negative remarks, videos, or pictures about faculty, students, community members, contest rivals, the schools, or the District.
    - Users may not publish any phone numbers, full names, email addresses or other confidential information of any students or employees for any reason.
    - In accordance with the District's JFCD Bullying Policy, users may not use social media sites to degrade, harass, bully, or discriminate against anyone.

**Penalties for Improper Use:**
The use of a District or State account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action, which may include suspension, expulsion, or criminal prosecution by government authorities. All discipline for misuse of District or State accounts or the Network will be determined on a per case basis by the appropriate administrator.

**Charges incurred by users while using the Network:**
Each user shall be responsible for any technology-related costs, fees, charges, or expenses incurred under that user's account in connection with the use of the Network except such costs, fees, charges, and expenses as the school district explicitly agrees to pay.

**Employee/District Responsibilities:**
- Employees will be held responsible for maintaining their District-assigned devices. Employees need to take care not to damage Network hardware assigned to them.
- The District will, when able, provide Accidental Damage Protection (ADP) for District hardware that is mobile (i.e. laptop, Chromebook, tablet) and assigned to an employee.
- Employees will run all updates on assigned District hardware within a timely manner of becoming available.
- Employees are responsible for the privacy of student information in conformity with FERPA and COPPA.
- The District (Technology Coordinator/Administration) is responsible for student protection online in accordance with CIPA and will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and/or harmful to minors over the Network.
- Students are not allowed, without strict supervision, to use employee-assigned devices or employees personal devices as these devices could allow access to material in violation of CIPA.
- Employees will be allowed use of District-assigned devices throughout the summer and other breaks.
- All expectations, restrictions, and responsibilities apply to personal devices that are connected to the Network except those referring specifically to District hardware.
- At the sole discretion of the District, devices may be offered for sale to the assigned user. The price will reflect the market value of the used device. Each device will be sold "As Is" and will be returned to its original purchased state (added software products removed). No warranties or service will be supplied on sold devices by the District, the District's administration, or other District employees.

**Student Responsibilities:**
Students will be held responsible for maintaining their 1:1 device and keeping them in good working order.

- Device batteries must be charged and ready for school each day.
- Only labels/stickers approved by the District may be applied to the device. This does not prohibit the user from obscuring cameras and microphones with non-permanent or easily-removed coverings that leave no residue.
- Devices that malfunction or are damaged must first be reported to the Technology Coordinator. The school district will be responsible for repairing devices that malfunction. Devices that have been damaged from normal use or accidentally will be repaired with no cost or minimal cost to the student. Students will be responsible for one-half the cost of repairs after damages of $100 have been accrued by that student, which may include one-half of the total replacement value of the device. Students will be entirely responsible for the cost of repairs or replacement to devices that are damaged intentionally.
- Students who have incurred $100 or more in accidental or intentional device damage may be asked to check their device in at the Office at the end of each day. Devices may be checked out again before classes begin the next day. Special permission to take a device home for work related to school can be given by the Principal.
- Stolen devices must be reported immediately to the Principal's Office and the police department.
- Individual school devices and accessories must be returned to the Technology Office at the end of each school year.
- Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment at De Smet for any other reason must return their individual school computer on the last date of attendance. If a student fails to return the computer at the end of the school year or upon termination of enrollment at DHS, that student will be subject to criminal prosecution or civil liability. The student will also pay the replacement cost of the computer. Failure to return the computer will result in a theft report being filed with the Kingsbury County Sheriff's Department.

**Guest Responsibilities:**
Guest users will be held responsible for maintaining any device assigned to them by the District. Damages to the device and charges related to the repair or replacement of the device will be billed to said guest user.
Guest users are also responsible for complying with COPPA and FERPA regulations to the extent each is legally given access to information relating to each regulation.

**User-created Data and Cloud Computing:**
Users will be provided with and use a State (K12) account to access email, support, and other cloud services. These will include but not limited to Microsoft Office 365, Microsoft OneDrive, Google Apps Suite, and Google Drive.
Employees are responsible for backing up data they create. Most employees will use either Microsoft OneDrive or Google Drive to do this. Some administrative employees will be given access to Network server space in order to save and backup District data.
Students will generally use Google Drive to store all user-created data. Students will also have access to and may be required to use Microsoft OneDrive.
Users are responsible for the content of their individual storage whether on an assigned device or in an assigned cloud storage drive (e.g. Google Drive). The District is not responsible for lost or compromised

data stored on devices or in the cloud. Users should take all precautions necessary to safeguard their credentials.

The use of cloud computing services to create and store data means that users of those accounts are solely-responsible for their individual cloud storage contents.

The District will not be responsible for any user-created data that may be lost when a device malfunctions, is damaged, or is being repaired.

Employees of the District may require or ask that students use or their accounts be linked to other online educational resources. All such resources will follow COPPA and FERPA regulations and will be first inspected and tested by an employee of the District. A non-comprehensive list of these resources is found below. The District will curate (here), to the best of its ability, all privacy statements for these resources.

| | |
|---|---|
| Google Apps Suite/Google Drive | GoGuardian |
| Microsoft Office 365/OneDrive | Scratch |
| SeeSaw | Adobe Spark |
| FlipGrid | NewsELA |
| Tinkercad | CodeCombat |
| CodeAcademy | Code.org |
| Promethean ActivCast | Promethean ClassFlow |
| Quizizz | Padlet |
| WriteAbout | Desmos |
| Fluency Tutor | Renaissance |
| IXL | BrainPop |
| Spelling City | StarFall |

**Computer Protection and User Costs:**

The District will assess technology charges to users based upon repair or replacement costs to damaged devices. Users are responsible for any damage to devices assigned to them by the District, unless it can be proven by the administration that the damage was caused by another and not the negligence of the assigned user. Current replacement value will be charged for lost or stolen devices. Once a user repair or replacement costs exceed $100 during a fiscal year, the user is responsible for one-half the cost of repair or replacement. These charges will include, but are not limited to, costs accrued from damage caused by liquid spills, accidental drops, power surges, natural disasters, fire, theft, loss, misuse, abuse, accidents, computer viruses, intentional or frequent damage, and cosmetic damage. Machine failures or faulty construction will be repaired or replaced at cost to the District or manufacturer.

# Student Photograph, Video, Interview, and Work Consent

The District and its employees or media members will, at times, post, print, or publish photographs or video of students in newspapers or magazines, or on approved social media (e.g Twitter, Facebook, or YouTube), employees' school-related websites, other non-profit education-related organizations' publications, or the school website (www.desmet.k12.sd.us) in a manner that will individually identify specific students. The District and its employees or media members will also, at times, post, print, or publish student work or student ideas (interviews) in any of the above methods. The use of student photographs, videos, and work is done in order to share student accomplishments, student experiences, and to promote the District. The District respects each individual's right to privacy and will act according to the directions from the parent/guardian.
Please select one of the following options:

- ❏ Yes, my child's photograph, video, work, and/or ideas may used in the manner described above.

- ❏ No, my child's photograph, video or any work may be displayed electronically or in print outside of the District's buildings.

If you have questions or concerns regarding this policy, please contact your building principal.

# Social Media Release

**In order to post pictures of your child, we need your permission.** These pages will publish photographs and relevant information about students for the purposes of informing the community about school and student activities. We consider online safety and privacy to be a priority. We would appreciate it if you would complete the permission slip at the bottom of this letter, which will determine if we can post images of your child on the Twitter / Facebook pages.

We will **NEVER** publish surnames, as we need to ensure the data of our children/families in school is protected at all times.

Whilst this is an amazing tool to communicate with parents and community members, it is unacceptable to violate the terms and conditions of the fair use policy by using slander and disrespecting the district's social media pages. The terms can be found on the Twitter / Facebook websites.

- ❏ **I give** permission to publish images and information about my child as described above.

- ❏ **I do not give** permission to publish images and information about my child as described above.

Parent/Guardian Name Printed _____

Parent/Guardian Signature: _____ Date: _____

# End User Acceptable Use Policy Acknowledgement of Understanding

The following agreement is valid for either 13 months from the date of signature or until September 15 of the succeeding school year, whichever constitutes a lesser time period.

**Student/Guardian:**

I have read and understand the District's AUP and agree that I am responsible for damages to the device assigned to me along with all charges assigned for damages or loss.

Student Name Printed _____
Student Signature: _____ Date: _____

I have read and understand the District's AUP and agree that the above named student is responsible for damages to their assigned device. I also agree to be responsible for all charges accrued for damages to the device of the above named student.

Parent/Guardian Name Printed _____
Parent/Guardian Signature: _____ Date: _____