Acceptable Network and Internet Use Policy
Stanley County School District 57-1

I. Introduction

The Children's Internet Protection Act (CIPA), 47 U.S.C. §254(h)(5) require public schools to implement certain measures and actions to ensure that students are restricted from accessing inappropriate materials online using school-owned computers. This District's Acceptable Network and Internet Use Policy (hereinafter "AUP") is intended to set forth the specific obligations and responsibilities of all users, including students and staff, who access the District's Network, and to ensure such use complies with the CIPA requirements.

"Network" is defined as any and all District owned computers, servers, hardware or software, the District's local area network, wireless access points, the Internet, Internet 2, the District intranet, email, chat rooms, other forms of direct electronic communications or other communications equipment provided by the District regardless of the physical location of the user. This AUP applies even when District provided equipment (laptops, tablets, etc.) is used on or off premises of District property.

II. Acceptable Use

The Network may be used only as a tool to support and advance the functions of the District as well as its curriculum and educational programs. Access to the District's Network is a privilege and not a right. Users of the Network are responsible for their behavior and communications over the Network and access to Network services will be provided only to those staff and students who agree to act in a considerate and responsible manner and in accordance with the District's Internet Safety Policy and this AUP.

Students may use the Network only in support of educational activities consistent with the educational objectives of the District. Faculty and staff may use the Network primarily in support of education and research consistent with the educational objectives of the District. Faculty and staff may access the Network for limited personal use but not for any commercial or business use; however, such personal use may not violate any applicable rules and regulations or applicable administrative procedures or interfere with job performance. Use of the Network must be in compliance with applicable laws, including all copyright laws and all materials on the Network should be presumed to be copyrighted.

All members of the staff who wish to use the Network must sign this AUP whenever requested by the District, to confirm that the staff person has read and understands this policy and agrees to abide by it. Each student must sign this AUP annually to confirm that the student has read and understands this policy and agrees to abide by it. Students who are under 18 must have their parents or guardians sign this AUP and submit it to the District.

III. E-mail

Students in grades 6-12 will be provided with a K-12 email address. Students should maintain high integrity with regard to email content. Students should check their email regularly. Student email is subject to inspection by school officials at all times. Always use appropriate language and don't transmit language/material that is profane, obscene, abusive, or offensive to others.

IV. Network Etiquette

Users are expected to abide by generally accepted rules of network etiquette (netiquette). These include but are not limited to:

A. Be polite. Do not send or encourage others to send messages that are abusive or otherwise fall in the definition of Prohibited Use in Section IV.
B. Use appropriate language. Remember you are a representative of your school on a non-private network. You may be alone on a computer but what you write can be viewed around the world. Do not swear, use vulgarities or any other inappropriate language.
C. All communications and information accessible via the Network should be considered private property that you cannot appropriate for your own use without appropriate attribution and consent.

V. Bring Your Own Device (BYOD)

No student shall bring their own personal or electronic mobile device (laptop, tablet, phone, iPad, etc.) and connect it to the school network. Students may be subject to discipline per **the Cell Phones and Portable Media Devices** policy outlined in the student handbook.

VI. Prohibited Use

The District reserves the absolute right to define prohibited use of the Network, adopt rules and regulations applicable to Network use, determine whether an activity constitutes a prohibited use of the Network, and determine the consequence of such inappropriate use. Prohibited use includes but is not limited to the following:

A. 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 or copyrighted materials;
B. Criminal activities that can be punished under law;
C. Selling or purchasing illegal items or substances;
D. The unauthorized collection of email addresses ("harvesting") of e-mail addresses from the Global Address List and other District directories;
E. Obtaining and/or using anonymous email sites; spamming; spreading viruses;
F. Circumvention of the District's Technology Protection Measure/FortiGuard filter to access blocked sites;
G. Disclosure of minors' personal information without proper authorization;

H. Students' disclosure of personal information such as the student's name, address, phone number, password or social security number, to other users when engaging in online activities including but not limited to chat rooms, email, social networking web sites.

I. Causing harm to others or damage to their property, such as:
   1. Using profane, abusive, or impolite language; threatening, harassing, bullying or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
   2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
   3. 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;
   4. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws; or
   5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".

J. Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
   1. Using another's account password(s) or identifier(s);
   2. Interfering with other users' ability to access their account(s); or
   3. Disclosing your own or anyone's password to others or allowing them to use your or another's account(s).

K. Using the network or Internet for Commercial purposes:
   1. Using the Internet for personal financial gain;
   2. Using the Internet for personal advertising, promotion, or financial gain; or
   3. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

VII. Off-Premise Use of Network

Students under the age of 18 should only access District-assigned email accounts and/or other Network components including but not limited to school-assigned computers such as laptops, tablets or e-readers off of District premises if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's off-premise use of the Network and ensuring such use complies with this AUP.

VIII. Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the Network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

IX. Enforcement

Prohibited use of the Network may, for students, result in disciplinary action up to and including suspension or expulsion from school or, for employees, suspension or termination of employment. Where circumstances warrant, prohibited use of the Network may be referred to law enforcement authorities.

PENALTIES: Unless under the direct supervision of a teacher:
First Offense: No computer use for two (2) weeks
Second Offense: No computer use for four (4) weeks
Third Offense: No computer use for the balance of the school year.

When a school administrator has a reasonable belief that a student has violated a school rule, policy or the law, and there are facts and inferences that would cause a reasonable person to suspect that a search of the student's personal technology device(s) will reveal evidence of a violation of said school rule, policy or the law, the administrator shall have the authority to search such device, provided that the scope of the search relates to the suspected violation giving rise to the reasonable suspicion.

Children's Internet Protection Act (CIPA)

All Internet activity will pass through the district's FortiGuard firewall and content filter, which is regularly monitored, by the Technology Coordinator as well as DDN. This appliance will provide protection to the internal network from outside intrusion and will provide content filtering of inappropriate sites.

The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. The Superintendent is delegated authority to implement these educational requirements.

Each user is required to sign the Acceptable Network and Internet Use Policy, which must also be signed by a parent or guardian before access to the Internet is granted.

Parents or guardians will give explicit permission for student photos and/or work to be posted on the school web page by signing the district Web Page Permission agreement.