NEWELL SCHOOL DISTRICT ACCEPTABLE NETWORK AND INTERNET USE

INTRODUCTION: The Children's Internet Protection Act (CIPA), 47 U.S.C. §254(h)(5) and South Dakota Consolidated Statutes Section 22-24-55 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.

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.

INTERNET SAFETY: It is the policy of the District to protect computer users from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator.

A. The organization has implemented a technology protection measure that blocks access to inappropriate matter such as child pornography, obscene materials, and material that is harmful to minors.
B. In order to protect the safety and security of its students, network users are prohibited from revealing personal information to other users when engaging in

online activities including but not limited to chat rooms, email, and social networking web sites.

C. All network users are prohibited from hacking and engaging in any unlawful online activity.
D. All network users are prohibited from disclosing or disseminating personal information without proper authorization regarding minors.
E. All network users are prohibited from accessing sites or online materials that are blocked by the technology protection measure.

TECHNOLOGY PROTECTION MEASURE: All school owned computers must be equipped with a technology protection measure. Adult users may request the Technology Protection Measure to be temporarily disabled in order to conduct bona fide research or for another lawful purpose. The Technology Protection Measure must be re-activated as soon as the adult finishes using the computer for the authorized bona fide research or other lawful purpose.

SIGNING OF THE POLICY: Each network user shall be required to sign an Acceptable Use Policy Agreement in the form prescribed by the Superintendent or his/her designee. This Agreement will be signed at the beginning of each school year.

MONITORING OF ONLINE ACTIVITIES: It shall be the responsibility of all personnel of this organization to monitor students' online activities and use of the network to ensure that their use is in compliance with CIPA and this policy.

CYBERBULLYING AND APPROPRIATE ONLINE EDUCATION: Students will be educated annually about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. The implementation of this provision is delegated to the Superintendent.

NETWORK ETTIQUITE: 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.

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/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.

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.

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.

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.

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.

_____	_____	_____
Parent/Staff Signature	Student Signature	GRADE
_____	_____	
Parent/Staff Name Printed	Student Name (Printed)	
_____	_____	
Date	Date	