Sioux Falls School District Student Teacher Technology Use Policy Agreement

The use of technology must be in support of education and research. Therefore, computer and network resource use must be consistent with the academic goals of the District, and follow the practice and protocols outlined in District Policy IJNDC-R and all other applicable policies. Furthermore; any user, staff, or teacher expectation outlined in the policy would be directly applicable to student teachers in the acceptable and ethical use of technology resources and protection of student information.

Policy IJNDC-R

Acceptable and Ethical Use of Technology Resources

Sioux Falls School District Network and Computer Systems and Wireless Access
The District's computer systems and networks ("District Network") are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available.

The use of the District Network, inclusive of the Wide Area Network (WAN) and the Local Area Network (LAN – includes wireless access) is a privilege, not a right. Persons using the District Network, regardless of whether the equipment used is personal or District provided, shall have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the District Network. All persons using the District Network regardless of whether the equipment used is personal or District provided, are governed by District Policies/Regulations.

Guidelines are provided to make all users aware of the responsibilities associated with educational, efficient, ethical, and lawful use of network resources. If a person violates any of these provisions, privileges may be terminated, access to the District Network may be denied, and the appropriate disciplinary action shall be applied. The District's discipline policy shall be applied to student infractions.

The District does not guarantee that the District Network will be uninterrupted or error-free; nor does it make any warranty as to the results to be obtained from use of the service or the accuracy or quality of the information obtained on or by the network. Access to the District Network is provided on an "as is" basis without warranties of any kind. Neither the District nor any of its agents or employees shall be liable for any direct, indirect, incidental, special, or consequential damages arising out of the use of or inability to use the District Network or out of any breach of any warranty.

Internet Safety
The District shall operate a technology protection measure that blocks or filters Internet access. The technology protection measure shall protect against access by adults and minors to content, including visual depiction that is abusive, obscene, profane, sexually explicit, threatening, and illegal or pertains to pornography or with respect to use of the computers by minors, other information that is harmful to minors. The District shall make every effort to restrict access to inappropriate materials and shall monitor the online activities of the end users. District staff may file a request with the Technology Integration Facilitator to unblock websites that they believe have significant educational value. If the website is determined to be appropriate, the site will be unblocked for educational purposes or bona fide research only.

To the extent possible, steps shall be taken to promote the safety and security of users of the District Network when using electronic mail, chat rooms, and other forms of direct electronic communications. Specifically, prevention of inappropriate network usage includes (1) unauthorized access, including so-

called “hacking,” and other unlawful activities; and (2) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

The District shall make every effort to restrict access to inappropriate materials and shall monitor the online activities of minors. The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyber-bullying awareness, prevention and response.

Security of the District Network is a high priority. Anyone observing a security problem on the District network shall notify District personnel. Any person identified as a security risk or having a history of problems with other computer systems may be denied access to the District Network.

Educational Use of District Technology Resources
Online communication and network resources are critical to 21st Century teaching and learning. The District Network and all technology resources are considered an extension of the classroom. An educator’s primary responsibility is to develop students who are fully prepared to communicate effectively, ethically and safely. Teachers will provide developmentally appropriate guidance to students using telecommunications and electronic information resources related to the District curriculum. Teachers may allow students to use forms of online collaboration such as email, wikis and blogs, etc. only for educational purposes and only with proper supervision. Proper supervision shall include the teachers having documentation of the identities of participating students and monitor the account. Any email account issued by District Staff is the property of the District and students have no expectation of privacy or confidentiality in the content of electronic communications sent to or from that email address. The District expressly reserves the right at any time to review the subject, content, and appropriateness of electronic communications reporting any violation to the school administration or law enforcement officials.

Acceptable Use of District Technology Resources:
Internet use by students for direct classroom instruction, e.g. where the teacher uses the Internet as a classroom demonstration or in a situation where the students are using computers and being supervised by District staff in the directed use of specific Internet sites as part of the class curriculum is allowed. Teachers should be prepared to provide alternate activities for students who have lost privileges through disciplinary action.

All user accounts are considered the property of the District. The District expressly reserves the right at any time to review the subject, content, and appropriateness of electronic communications or other computer files and remove them if warranted, reporting any violation to the school administration or law enforcement officials.

Disciplinary action may be taken against students whose electronic communications cause a substantial disruption to the education environment or interfere with another student’s rights. Criminal action may be taken against students if their electronic communications constitute a threat.

The District’s Network may not be used for personal gain, which includes District email and/or web pages, to solicit sales or conduct business.

Proper Use of District Network and Computer Systems
Proper use of the District Network requires that District staff and students abide by the following guidelines. District staff and students shall:

a. be responsible for all use of the networks under their accounts, regardless of whether access is gained with or without the person’s knowledge and/or consent;

b. immediately notify the District if the person suspects any unauthorized use of their account. The person shall remain liable and responsible for any unauthorized use until the District is notified of the suspected unauthorized use and has a reasonable opportunity to act upon such notice;
c. be responsible for any costs, fees, charges, or expenses incurred under the person's account number in connection with the use of the network except such costs, fees, charges, and expenses as the District explicitly agrees to pay;
d. avoid anonymity when communicating through electronic resources, unless authorized by the District or completing professionally-related surveys;
e. develop web-based content only to fulfill course or school-related activity; web pages shall include an identifiable image of a student with or without association to the student's name, school, or program only if written authorization has been obtained from the student's parent or guardian through the District's registration form; Annual Emergency Health, Student Update and Authorizations form; or other written consent;
f. ensure that student information shared electronically complies with the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act, as well as District student records policy JRA/JRA-R;
g. delete non-District authorized or adopted software if disk-space or system conflict issues arise;
h. abide by all District policies and regulations when accessing personal email accounts, chat rooms, social networking sites or other forms of direct electronic communications via the District's Network;
i. not send, access, or retain any abusive, defamatory, obscene, profane, sexually explicit, pornographic, threatening, or illegal material;
j. not transmit copyrighted material without the express consent or authorization of the owner of the copyrights;
k. not disclose passwords except to authorized District staff;
l. be responsible for damages or the cost of correcting any damage to the District Network, District equipment or software or attempts to harm or destroy data of another person. This includes, but is not limited to, "hacking" or creating, loading, or sharing malicious software, scripts or code (e.g. executable files (*.exe), batch files (*.bat), command files (*.com), system files (*.sys)). ;
m. not install equipment on or make modifications to the District's Network, or download free or paid-for online educational services, or applications, which might utilize protected student information, without pre-authorization from the Director of Technology and Information Services;
n. not utilize proxy sites or other means to circumvent the District's filter;

Ethical Use of District, Public, or Private Technology Resources
Ethical behavior requires that District staff and students show consideration and respect whenever using computers or electronic communication/technology/devices/resources. When interacting with each other, District staff and students shall:

a. not include in electronic communication between staff, students and/or parents/guardians, comments or content that would not be acceptable in a face-to-face communication;
b. not disclose, use, or disseminate unauthorized personal information of another person;

c. distinguish between personal social networking sites and professional social networking sites. Staff shall not invite or accept current District students, except for the staff person's relatives, into any personal social networking sites; and
d. evaluate all information for its accuracy, reliability, and authority.

District Protection of Student Personally Identifiable Information
The District allows the use of online and cloud-based services and applications that are educationally appropriate. When such services may utilize personally identifiable information, the District must ensure the provider agrees to protect such information before District staff or students use the service or disclose any student information.

When the District provides student data to providers for use of online educational services, all data created by students, teachers, and staff, related to students, will be considered personally identifying information protected by the Family Educational Rights and Privacy Act (FERPA). Personally identifying information includes specific identifiers such as name, address, or student number, and any information, alone or combined, that may allow someone to identify the student with reasonable certainty. In order to protect personally identifying information, the District shall enter into written agreements with third party vendors or service providers and these agreements shall include satisfactory assurances that the provider will appropriately safeguard any personally identifying information in accordance with state and federal laws. At a minimum, any agreement shall include terms that 1) ensure the provider uses the information for authorized purposes only; 2) prevents disclosure of protected student information by the provider to other third parties; 3) maintains that student data collected by the provider is under the direct control of the District with regard to the provider's use of that information; and 4) requires the provider to observe state and federal laws for the use, and breach, of personal identification information. When a provider requires the user to accept the providers' standard 'terms of service' agreement (TOS), the District will review the TOS to ensure the provider will protect personally identifying information before allowing use of the service, or application, by staff and students.

To prevent inadvertent disclosure, all free and paid-for online educational services, or applications, to be used either on District computers or personally owned devices, which might utilize personally identifying information, must be reviewed and approved by the Director of Technology and Information Services prior to use by staff and students.

If, for any reason, a provider plans to use personally identifying information for its own commercial or marketing purposes, the District shall obtain parental consent before disclosing such information.

Discipline
Disciplinary action may be taken against staff or students whose communications (on or off-site) constitute a threat and cause a substantial disruption to the education environment or substantially interferes with another's rights. Criminal action may be taken if the communication constitutes a threat.

Legal References:

Children's Internet Protection Act (CIPA) 29 USC § 6777; 45 CFR §54.520
Children's Online Privacy Protection Act (COPPA) 15 USC §6501-6506
Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 1232g; 34 C.F.R. Part 99
Protection of Pupil Rights Amendment 20 U.S.C. §1232h; 34 C.F.R. Part 98

Related Policies/Regulations:

GBEB – Code of Conduct
JK/JK-R – Student Discipline, Suspension and Expulsion
JRA/JRA-R – Student Records

The student teacher's internet and email use can be tracked and monitored. Files on any of the Sioux Falls School District's computers, data servers, or approved cloud storage services are property of the District, and therefore, subject to inspection. The signature of the student teacher acknowledges the understanding of this agreement, and all the applicable District Policies.

Please print legal name:

First Name Middle Name Last Name

Student Teacher's Signature:

Date: _____