IIBF-E

Fremont County School District #1
Student Network and Internet Acceptable Use Agreement

Fremont County School District #1 strongly believes in the educational value of the Internet and other online information resources. They can increase the power of curriculum content standards, enable exciting collaborations, increase productivity, and improve student learning. Resources provided by the Internet and other media sources are important parts of the District's instructional program. These services are provided to promote educational excellence in schools, support our curriculum, and support individual academic needs. **Student use of District computers, networking, or applications constitutes acceptance of the conditions within this agreement as well as additional stipulations within the school's student handbook**.

General Statement: Individual Responsibility of Parents and Users
Even though filtering and other protection are in place on the District network, all users and their parents/guardians are advised that access may include the potential for access to materials inappropriate or offensive for school-aged pupils. All users are responsible for their use of technology resources and the Internet. The District does not accept responsibility for students accessing inappropriate content or acting contrary to this agreement.

General Statement: No Expectation of Privacy
Network and Internet access is provided as a tool for education. The District reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the district computer network and Internet access and any and all information transmitted, received, or stored in connection with such usage. All such content shall become and remain the property of the District, and no student shall have any expectation of privacy regarding such materials. The District may share such transmissions with the student's parent/guardians, law enforcement, and other entities that the District deems necessary.

Student Account Usage
Each student is given a unique identifying network account and password. These credentials are private and to be used only by that student. Students are responsible for their individual accounts and the actions on their network accounts. Students should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should students provide their password to another student. If a student suspects her/his network account credentials has been compromised, the student should immediately inform a teacher or other staff member so action can be taken to protect her/his account.

Internet Use Filtering and Monitoring
To comply with federal law, the District employs several methods of Internet content filtering and monitoring. However, no Internet content filtering system can be fully effective in preventing access to harmful and inappropriate material. With global access to computers and people, there is a risk that students may access material that may not be considered to be of educational value in the context of the school setting. Students receive instruction, appropriate to their age, regarding strategies to avoid the inadvertent access of inappropriate material and what to do if they accidentally access such material. Users will not use District resources to view or otherwise gain access to potentially objectionable materials. This includes text materials, video, images, or sound files that may be considered objectionable in an educational setting. If students mistakenly access inappropriate information, they should immediately disclose this access to their teacher or other supervising staff member. If a student finds that other users are visiting offensive or harmful sites, she/he should report such use to her/his supervising teacher.

Student File Storage
All students, as part of their network account, are given storage space both on a school server as well as through an online service (see below). Storage space is set aside for educationally-appropriate content as well as student work. The District reserves the right to inspect any material stored in files to which users have access and will edit or remove any material which the district staff, in its sole discretion, believes may be objectionable. Music files, videos files taking a large amount of storage, and other non-educational material may be deleted at any time without notice to the student.

Student Email and Offsite File Storage Usage
All students in grades 6-12 are given private District-managed email accounts and network "cloud" storage. These accounts are available to students both at school and offsite (home, library, etc). These accounts are hosted by a third-party service chosen by the District and specifically geared toward educational users (Microsoft Live@Edu). Email accounts may at any time be monitored by authorized school and District staff and may be shared with district administration, law enforcement, parents/guardians, and others as necessary. If a student suspects her/her email account has been compromised, she/he should immediately inform a teacher or principal. Students should not delete any threatening or suspicious messages, but leave them as evidence for authorized personnel to evaluate.

Social Networking Usage and Website Posting
The use of social networking and collaborative sharing sites is limited to District-approved online applications, such as Edmodo and Wikispaces. Student accounts in approved applications are monitored and managed. Students may be invited to participate in various publishing and Internet posting opportunities through the District (such as online video, newsletters, wiki editing). The use and sharing of such resources and information online will fall under expectations within this agreement as well as school-wide and District expectations.

Expectations Regarding Usage and Communication
The same rules and expectations that students have regarding communication and interaction with peers and with staff apply to online communications.

- Students shall not access, post, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, educationally inappropriate, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion, or political beliefs.
- Students shall not use the system to promote any activity prohibited by school or district policy, local law, state law, federal law, or Fremont #1 Board policy.
- Students shall not disrupt, vandalize, or modify any network equipment, software, or computer hardware.
- Students shall not interfere with the work of other users or violate the privacy of others.
- Students shall not knowingly introduce malware, worms, keyloggers, or other malicious software into the network or onto an individual computer.
- Students shall not download or install executable software without the direct approval of authorized staff.
- Students shall not attempt to compromise or bypass content filtering and other security measures.

Schools and/or teachers may impose other guidelines and rules in addition to those in this document. Disciplinary consequences for violation of this agreement may include classroom sanctions that are defined by teacher, and/or school-wide sanctions including limited or no access to technology at the school as well as other consequences deemed appropriate by school and/or District administration.

BYOD ("Bring Your Own Device") guidelines
A growing number of students are bringing personal technology – such as Internet-connected smartphones, netbooks, and mobile PDAs – to use during the school day on the guest wireless network provided by the school. Devices that connect to the Fremont #1 guest wireless network are subject to the same usage expectations and rules as are District-owned devices, and also subject to additional limitations established by the teacher/school. The District takes no responsibility for any issue or loss arising from the use of personal devices. The District reserves the right to search any and all personal technology devices brought upon the school campus or to any school activity or on any school bus if in the judgment of the supervisor or administrator in charge there is a reasonable suspicion to believe it contains evidence of the violation of a District rule, policy, or state or federal law which could subject the student to discipline.

Opt-Out
Due to the pervasive and immersive use of technology in our District, it has become impossible for students to "opt-out" of using Internet resources. In extraordinary situations, the parents and principal can choose to limit some Internet access for a student, but exceptions will always be made for Internet access to testing, student email, and other educational applications that are required parts of our curriculum, daily classwork, and communication.

Disclaimer
Fremont County School District #1 makes no warranties of any kind, whether expressed or implied, for the technology and Internet services it is providing. The District will not be responsible for any damages suffered by users, including loss of data resulting from delays, non-deliveries, incorrect deliveries, or service interruptions caused by its own negligence, user errors, omissions, or factors beyond the control of the District. Use of any information obtained via the Internet is at the user's own risk for the user's own purpose. The District specifically denies any responsibility for the accuracy or quality of information obtained through its Internet access. The district does not warrant that the functions of the system will meet any specific requirements or that it will be error-free or uninterrupted. The District shall not be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or monetary loss) sustained or incurred in connection with the use, operation, or inability to use any aspect of the system or service.

Signature
My signature below indicates I have read and agree to adhere to these usage guidelines and restrictions.

_____	_____	_____
Signature	Printed name	Date