Herscher Community Unit School District #2

Computer/Internet Acceptable Use Policy

The following document is pursuant with Board Policy 6:235

Please read this document carefully and completely before signing.

Acceptable Use:

All Users of the District Technology ("System") must comply with this Acceptable Use Policy and Guidelines contained within, as amended from time to time.

The System shall be defined as any and all computer hardware and software, owned or operated by the district, the district electronic mail, the district web site, and the district online services and bulletin board system. "Use" of the System shall include use of or obtaining access to the System from any computer terminal whether or not it is owned or operated by the district.

Users have no expectation of privacy in their use of the System. The district has the right to access, review, copy, delete, or disclose, as allowed by law, any message sent, received, or stored on the district's electronic mail system. The district has the right to and does monitor the use of the system maintenance and to determine whether the use is consistent with Federal and State laws and district policies and guidelines.

Prohibited Use:

The System shall not be used to:

1. Engage in activities which are not related to district educational purposes or which are contrary to the instructions from supervising district employees;
2. Access, retrieve, or view obscene, profane, or indecent materials. ("Indecent materials" are those materials which, in context, depict or describe sexual activities or organs in terms blatantly offensive, as measured by contemporary standards. "Obscene materials" are those materials which, taken as a whole, appeal to the voyeuristic interest in sex, which portray sexual conduct in a blatantly offensive way in which taken as a whole, do not have any serious literary, artistic, political or scientific value.)
3. Access, retrieve or disseminate any material in violation of any Federal or State laws or regulation or district policy or rule. This includes, but is not limited to, improper use of copyrighted material, improper use of the System to commit fraud, improper use of passwords or access codes, or disclosing the full name, home address or phone number of any student, staff member or System user.
4. Transfer any software to or from the System without authorization from System administrator.
5. Engage in for profit or non school-sponsored commercial activities, including advertising or sales.
6. Harass, threaten, intimidate, or otherwise demean an individual or group of individuals based on sex, color, race, religion, disability, national origin or sexual orientation.
7. Disrupt the education process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either before, during or after school hours.
8. Disrupt or interfere with the System.
9. Gain unauthorized access to or vandalize the date or files of another System user.
10. Gain unauthorized access to or vandalize the System or the technology system of any other individual or organization.
11. Forge or improperly alter e-mail messages, use an account owned by another user, or disclose another user's password.
12. Invade the privacy of any individual, including Federal or State laws regarding limitations on the disclosure of student records.
13. Download, copy, print or otherwise store or possess any data which violates Federal or State copyright laws or these enclosures guidelines.
14. Send nuisance e-mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other welcoming messages.
15. Send nuisance e-mail to multiple users without prior authorization by the appropriate district administrator.
16. Conceal or misrepresent the user's identity while using the System.
17. Post material on the district's website without the authorization of the appropriate district administrator.

The use of the System for any of the above may result in discipline or other consequences as provided in these guidelines and the district's Discipline Code and Rules.
Please note that while extensive, the above list is not all-inclusive.

Herscher Community Unit School District #2

Computer/Internet Acceptable Use Policy

Privileges:
Access to the System is provided as a privilege by the district and may be revoked at any time. Inappropriate use may result in discipline, including loss of System use privileges.

The System, including all information and documentation contained therein is the property of the district except as otherwise provided by law.

Personnel Handling Credit Card Information:
All cardholder hardcopy data should be destroyed once it is no longer needed.

- The hardcopy materials should be destroyed (e.g. shredded, incinerated, pulped, etc.) such that reconstruction is not practically possible.
- Any materials that are not immediately destroyed (e.g. are placed in a to-be-shredded container), need to be secured.

Student Created Websites/Photo Release:
Any website created by a student using the System must be part of a district- or school- sponsored activity, or otherwise authorized by the appropriate district administrator.

All content, including links, of any website created by a student using the System must receive prior approval by the classroom teacher or an appropriate district administrator. All contents of a website created by a student using the System must conform to this policy and these guidelines.

At various times, photographs are taken of students while they are in educational setting at the school. These pictures may be used in district publications including electronic formats and may also be released to local news media. Parents should notify the school in writing if they do NOT want their child's photograph used for such purposes.

Security and User Reporting Duties:
Security in the System is high priority and must be treated as such but all users. Students are prohibited from sharing their log-in IDs and/or passwords with any other individual. Any attempt to log-in as another user may result in discipline. A user who becomes aware of any security risk or misuse of the System, should immediately notify a teacher, administrator or other staff member.

Vandalism:
Vandalism or attempted vandalism to the System is prohibited and may result in discipline as set forth in these guidelines and potential legal action. Vandalism includes, but is not limited to, knowingly downloading, uploading, or creating computer viruses as well as physically damaging district hardware (e.g. computers, keyboards, mouse, etc.)

Disclaimer:
The Herscher CUSD#2 makes no warranties of any kind, expressed or implied for the System. The district is not responsible for any damages incurred, including the loss of data resulting in delays, non-deliveries, mis-deliveries, or service interruptions. Use of any information obtained via the System is at the user's risk. The district is not responsible for the accuracy or quality of information obtained through the System. The district is not responsible for any user's intentional or unintentional access of material on the internet which may be obscene, indecent or of inappropriate nature.

Discipline/Consequences for Violations:
A student or staff member who engages in any of the prohibited acts listed shall be subject to:

1. suspension or revocation of System privileges,
2. other discipline including suspension or expulsion from school (students),
3. referral to the law enforcement authorities or other action in appropriate cases.

Misuse of the System by a student may be considered gross misconduct and a student may be subject to discipline pursuant to the Student Discipline Policy. A student who believes his/her privileges have been wrongfully limited may request a meeting with the building principal to review the limitation.

Herscher Community Unit School District #2

Computer/Internet Acceptable Use Policy

Employee Use of Social Media Sites, including personal sites

Because of the unique nature of social media sites, such as Facebook and Twitter, and because of the district's desire to protect its interest with regard to its electronic records, the following rules have been established to address social media site usage by all employees:

KEEP PERSONAL AND PROFESSIONAL ACCOUNTS SEPARATE

Staff members who decide to engage in professional social media activities will maintain separate professional and personal email addresses. Staff members will not use their district email address for personal social media activities. Use of district email for this purpose is prohibited and will be considered a violation of district policy that may result in disciplinary action.

CONTACT WITH STUDENTS

Although it is desired that staff members have a sincere interest in students as individuals, partiality and the appearance of impropriety must be avoided. All staff shall maintain a professional relationship with all students, both inside and outside of the classroom. Listing current students as friends on networking sites wherein personal information is shared or available for review is not recommended. Contacting students through electronic means is to be school-related and generic. Inappropriate contact of any kind, including via electronic media is prohibited.

Nothing in this policy prohibits district staff and students from the use of education websites and/or use of social networking websites created for curricular, co- curricular, or extra-curricular purposes where professional relationship is maintained with the student. Failure to maintain a professional relationship with students, both inside and outside of a classroom setting, including interaction via social networking websites of any nature, e-mailing, texting, communication-specific apps, or other electronic methods may result in disciplinary action up to and including termination.

RULES CONCERNING DISTRICT-SPONSORED SOCIAL MEDIA ACTIVITY

If an employee wishes to use Facebook, Twitter, or other similar social media sites to communicate meetings, activities, games, responsibilities, announcements, etc. for a school-sponsored club or a school-based activity or an official school-based organization, the employee shall comply with the following procedures and rules:

Notify the District

Employees that have or would like to start a social media page should contact their building administrator and/or superintendent. All district pages must have an appointed employee who is identified as being responsible for content. The building administrator and/or superintendent should be aware of the content on the site, arrange for periodic monitoring of the site, and for the receipt and response to complaints about the content on the site. The superintendent reserves the right to shut down or discontinue the site if he/she believes it is in the best overall interest of the students and/or district.

Have a Plan

District staff will consider their messages, audiences, and goals, as well as strategy for keeping information on social media sites up-to-date, accurate, and in the best interest of our students.

Protect the District

Posts on district-affiliated social media sites should protect the district by remaining professional in tone and in good taste. Carefully consider the naming of pages or accounts, selection of pictures or icons, compliance with district policy, state, and federal laws with regard to student and employee confidentiality, and the determination of content. The employee must also comply with the following rules:

1. The employee must set up the club, etc. as a group list that will be closed and moderated.
2. The employee must set up mechanisms for delivering information to students that are not members of the group via non-electronic means.
3. Members will not be established as friends but as members of the group list.
4. Anyone who has access to the the communications conveyed through the site may only gain access by the permission of the employee (e.g. teacher, administrator, or supervisor). Persons desiring to access the page may join only after the employee invites them and allows them to join.

5. Parents shall be permitted to access any site that their child has been invited to join. Parents shall report any communications they believe to be inappropriate by students or school personnel to administration.
6. Access to the site may only be permitted for educational purposes related to the club, activity, organization or team.
7. The employee responsible for the site will monitor it regularly.
8. The employee's supervisor shall be permitted access to any site established by the employee for a school-related purpose.
9. Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all district-sponsored social media activity. This includes maintaining a separation between the school activity pages and employees personal social media profiles and pages.
10. Postings made to the site must comply with all other district policies pertaining to district web sites, internet usage, technology and confidentiality of student information.

Personal Sites

The board respects the right of employees to use social media as a medium of self expression on their personal time. As role models for students, however, employees are responsible for their public conduct even when they are not performing their job duties as employees of the district. Employees will be held to the same professional standards in their public use of social media and other electronic communications as they are for any other public conduct. Further, school employees remain subject to applicable state and federal laws, board policies, administrative regulations and applicable code of ethics, even if communicating with others concerning personal and private matters. If an employee's use of social media interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

Employees are responsible for the content on their social media sites, including content added by the employee, the employee's friends or members of the public who have access to the employee's site, and for web links on the employee's site. If you identify yourself as a district employee online, it should be clear that the views expressed, posted, or published are personal views, not necessarily those of the district, it's Board, employees, or agents.

Opinions and/or other content expressed or posted by staff on a social networking website have the potential to be disseminated far beyond the speaker's desire or intention, and could undermine the public perception of the individual's fitness to educate students, and thus undermine teaching effectiveness. In this way, the effect of the expression and publication of opinions or other content could potentially lead to disciplinary action being taken against the staff member, up to and including termination or non-renewal of the contract of employment.

Posting to Social Media Sites

Employees who use social media for personal purposes must be aware the content they post may be viewed by anyone, including students, parents and community members. Employees shall observe the following principles when communicating through social media:

1. Employees shall not post confidential information about students, employees or school system business;
2. Employees are encouraged not to accept current students as friends or 'followers' or otherwise connect with students on social media sites, unless the employee and student have a family relationship or other type of appropriate relationship that originated outside of the school setting.
3. Employees shall be professional in all internet postings related to or referencing the school system, students, and other employees.
4. Employees shall not use profane, pornographic, obscene, indecent, lewd, vulgar or sexually offensive language, pictures or graphics or other communication that could reasonably be anticipated to cause a substantial disruption to the school environment.
5. Employees shall not use the school system's logo or other copyrighted material of the system without express, written consent from the board.
6. Employees shall not post identifiable images of a student or student's family without permission from the student and the student's parent or legal guardian.
7. Employees shall not use internet postings to libel or defame the board, individual board members, students or other school employees.

8. Employees shall not use internet postings to harass, bully or intimidate other employees or students in violation of district policy.
9. Employees shall not post inappropriate content that negatively impacts their ability to perform their jobs.
10. Employees shall not use internet postings to engage in any other conduct that violates board policy and administrative procedures or state and federal laws.
11. Employees are strongly discouraged from communicating with students, or parents regarding a student, from a personal e-mail account.
12. Employees shall be responsible for all content posted on their site by themselves and others and shall regularly monitor their site and remove any content that could reasonably be anticipated to cause a substantial disruption to the school environment.

Employees are to refrain from posting to personal social media pages (i.e. Facebook, Twitter) during the course of their paid work time, except for work-related duties.

Consequences – School system personnel shall monitor online activities of employees who access the internet using school technological resources. Any employee who has been found by the Superintendent or his/her designee to have violated this policy may be subject to disciplinary action, up to and including dismissal.

Protect Confidential and Proprietary Information – Employees shall not post confidential or proprietary information about the district, its employees, students, agents, or others. The employee shall adhere to all applicable privacy and confidentiality policies adopted by the district or as provided by state or federal law.

Do Not Use District Name, Logos or Images – Employees shall not use the district logos, images, iconography, etc. on personal social media sites; nor shall employees use the district name to promote a product, cause or political party, or political candidate; nor shall employees use personal images of students, names or data relating to students, absent written authority of the parent of a minor or authority of an adult or emancipated student.

Herscher Community Unit School District #2

Computer/Internet Acceptable Use Policy

Teacher / Staff
Signature Page

_____	_____	_____
Teacher/Staff (Print)	Building	Title

I have read and understand the above AUP. I understand that when I am using the internet or any other communication environment any day or time (24/7), I must adhere to all rules of the Acceptable Use Agreement.

I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be instituted.

I understand that Herscher CUSD #2 is not responsible for any damage or loss associated with a device which is not the property of the Herscher CUSD#2. Technology devices within the School building will be used to promote educational excellence and within the guidelines of this policy.

_____	_____
Teacher/Staff Signature	Date