FUSD-Technology Use Policy

Responsible Use Policy (RUP)

Access to Ferndale Unified School District's (FUSD) network is a privilege, not a right. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary. In particular, students will be held accountable for their actions and are encouraged to report any accidental use immediately to their teacher or school administration.

Students should not expect that files and communication are private. FUSD reserves the right to monitor student's online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of property, network and/or Internet access or files, including email.

Best Practices for Use

These are examples of inappropriate activity on the network, but reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the network, Users, schools, network or computer resources; 2) that expend resources on content it determines lacks legitimate educational content/purpose, or; 3) other activities as determined by as inappropriate.

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

1. Criminal activities that can be punished under the law
2. Selling or purchasing illegal items or substances
3. Obtaining and/or using anonymous email sites, spamming, spreading viruses
4. Causing harm to others or damage to their property
5. Using profane or abusive language; threatening, harassing, or making damaging or false statements about others; accessing, transmitting, or downloading offensive, harassing, or disparaging materials
6. Sharing and/or sending confidential information such as, but not limited to, testing materials
7. Deleting, copying, modifying, or forging other Users' names, emails, files or data, disguising one's identity, impersonating other Users; sending anonymous email
8. 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
9. Using any computer/mobile devices to pursue "hacking", internal or external to , or attempting to access information protected by privacy laws.
10. Accessing, transmitting or downloading large files maliciously including "chain letters" or any type of "pyramid schemes"
11. Using web sites, email, networks, or other technology for political uses or personal gain
12. Intentionally accessing, creating, storing or transmitting material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others
13. Advertising, promoting non- sites or commercial efforts and events
14. Using the network for non-academic related band-width intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities

Cybersafety and Cyberbullying

Staff shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

All Users

Despite every effort for supervision and filtering, all Users and Students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every User must take responsibility for his or her use of the network and make every effort to avoid such content. Every User must report security or network problems to a teacher, administrator, or system administrator.

Personal Safety

In using the network and Internet, Users should not reveal personal information such as home address or telephone number.

Confidentiality of User Information

Users should never give out private or confidential information about themselves or others on the Internet.

Active Restriction Measures

FUSD will utilize filtering software or other technologies to prevent Users from accessing visual depictions that are (1) obscene; (2) pornographic, or; (3) harmful to minors. Attempts to circumvent or 'get around' the content filter are strictly prohibited, and will be considered a violation of this policy. FUSD will also monitor the online activities of Users through direct observation and/or other technological means.

Online Tools

Technology provides an abundance of opportunities for Users to utilize interactive tools and sites on public websites that benefit learning, communication, and social interaction.

Users may be held accountable for the use of, and information posted on these sites if it detrimentally affects the welfare of individual Users or the governance, climate, or effectiveness of the school. From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge, are legitimate and safe. As the site is "public", the teacher is not in control of it; therefore, all Users must use their discretion when accessing information, storing, and displaying work on the site. All terms and conditions in this RUP also apply to User-owned devices utilizing the network.

Student Use of Online Tools

Online communication is critical to the students' learning of 21st Century skills, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression. Student safety is the primary responsibility of teachers.

Therefore, teachers need to ensure the use of Google Documents, classroom blogs, student email, podcast projects, email chat features, or other online tools follow all established Internet safety guidelines including:

- Students using online tools such as, but not limited to, Docs, blogs, podcasts are considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other online tools. This includes, but is not limited to, profane, racist, sexist, or discriminatory remarks.
- Students using Google Docs, blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
- Students should NEVER post personal information on the web (including, but not limited to, last names, personal details such as address or phone numbers, or photographs).
- Students should NEVER, under any circumstances, agree to meet someone they have met over the Internet.
- Any personal blog a student creates in class is directly linked to the class blog, which is typically linked to the student profile and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use the blog login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and should follow these guidelines.
- Students should NEVER link to web sites from their blog or blog comments without reading the entire article to make sure it is appropriate for a school setting.
- Students using such tools agree to not share their username or web posting spaces as classroom spaces. Speech that is

inappropriate for class is also inappropriate for a blog.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Student Supervision and Security

FUSD does provide content filtering controls for student access to the Internet using ' network as well as reasonable adult supervision. But, at times, inappropriate, objectionable, and/or offensive material may circumvent the filter, as well as staff supervision, and be viewed by students. Students are to report the occurrence to their teacher or the nearest staff member. Students will be held accountable for any deliberate attempt to circumvent technology security and supervision.
Students may not record or videotape within the classroom or on campus without first receiving permission from their teacher or administration.

Students using mobile and cellular devices while at school, during school-sponsored activities are subject to the terms and conditions outlined in this document and are accountable for their use.

Family Education Right and Privacy Act ("FERPA") Notification

The Family Educational Rights and Privacy Act ("FERPA") affords parents and students over 18 years of age ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days of the day FUSD receives a request for access. Please note that the California Education Code permits access within 5 days of the request.

   Parents or eligible students should submit to the school Principal, a written request that identifies the record(s) they wish to inspect. The Principal will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected. A student's education records will be available for review during the regular business hours of the school day.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.
   Parents or eligible students who wish to ask FUSD to amend a record should write FUSD clearly identify the part of the record they want changed, and specify why it should be changed. If FUSD decides not to amend the record as requested by the parent or eligible student, FUSD will notify the parent or eligible student of the decision and advise them of their right to a hearing regarding the request for amendment.

   Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. The right to provide written consent before FUSD discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

   One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel). A school official also may include a volunteer or contractor outside of the school who performs an institutional service or function for which FUSD would otherwise use its own employees and who is under the direct control of FUSD with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

   Upon request, FUSD discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer.

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by FUSD School to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

   Family Policy Compliance Office
   U.S. Department of Education
   400 Maryland Avenue, SW
   Washington, DC 20202-8520

5. FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, §99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from a student's education records without obtaining prior written consent of the parents or the eligible student –
   - To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(2) are met. (§99.31(a)(1))
   - To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))
   - To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the State educational agency in the parent or eligible student's State (SEA). Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)
   - In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))
   - To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))
   - To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))
   - To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))
   - To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))
   - To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9)) ● To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10)
   - Information FUSD has designated as "directory information" under §99.37. (§99.31(a)(11))
   - To an agency caseworker or other representative of a State or local child welfare agency or tribal organization who is authorized to access a student's case plan when such agency or organization is legally responsible, in accordance with State or tribal law, for the care and protection of the student in foster care placement. (20 U.S.C. § 1232g(b)(1)(L))
   - To the Secretary of Agriculture or authorized representatives of the Food and Nutrition Service for purposes of conducting program monitoring, evaluations, and performance measurements of programs authorized under the Richard B. Russell National School Lunch Act or the Child Nutrition Act of 1966, under certain conditions. (20 U.S.C. § 1232g(b)(1)(K)

Acknowledgement

This is to acknowledge that I have received an electronic copy of the Technology Use Policy.

Student ID# _____ **Grade**: _____

_____	_____	_____
Name (Printed)	Student Signature	Date
_____	_____	_____
Parent/Guardian Name (Printed)	Parent/Guardian Signature	Date