Student-Technology Acceptable Use Agreement

In accordance with Children's Internet Protection Act [CIPA]

BP 6163.4

The Governing Board intends that technological resources provided by the district be used in a responsible and proper manner in support of the instructional program and for the advancement of student learning. The Governing Board does not authorize the use of any computer equipment, network services, and online resources that are not conducted strictly in compliance with this policy. **Your signature on this document indicated that you have read the terms and conditions carefully, understand their significance, and agree to act responsibly.**

Before using the district's online resources, each student and his/her parent/guardian shall sign and return an Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree to not hold the district responsible and shall agree to indemnify and hold harmless the district and all district personnel for the failure of any technology protection measures, violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

The Governing Board believes that the use of computing devices in the learning environment, whether District-owned or personal (Bring Your Own Device), and access to online content via the Internet offer valuable resources for students and staff. The District goal in providing these resources is to promote educational excellence in schools by facilitating learning through collaboration, innovation, communication, access to knowledge and information, digital citizenship, and responsible use.

Technical limitations: **All network and Internet access at District facilities, regardless if the device is District-owned or personal (BYOD), will be content filtered for appropriate educational use.** The District makes careful and reasonable efforts to filter harmful content from students and that technology resources are used primarily for activities that support learning objectives. However, Internet content filtering is not an exact science and parents/guardians are advised that on occasion through intended use, or through deliberate and determined actions, a user may be able to gain access to content and services on the Internet which the District has not intended for educational purposes, or that may be considered inappropriate, offensive, or controversial. Parents are also advised that the District is not able to censor all communications on the Internet, nor control or filter content accessed by personal devices that utilize wireless carrier data networks. Parents/Guardians assume this risk by consenting to allow their students to participate in the use of computing devices and online services for the intended purpose of enhancing and accelerating learning.

Online/Internet Services: User Obligations and Responsibilities

Network access and Internet use is a privilege, not a right. Students who violate or disregard the Student Technology Acceptable Use Agreement and regulations may have their use privileges suspended or revoked and may be subject to other disciplinary actions. Students are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, the user obligations and responsibilities specified below, and the district's Student-Technology Acceptable Use Agreement.

Responsibility and Digital Citizenship

As a user of the Eureka Union School District network and technology resources:

1. I will use technology resources safely, responsibly, and primarily for academic purposes only (projects, homework, and school-related functions). I will bring the fully-charged device to school every day.
2. I understand that I am responsible for the proper care of my personal device, including any costs of repair, replacement, or any modifications needed to use the device at school.
3. I will follow instructions, respect guidelines, and use technology resources in the classroom as directed by my teacher.
4. I will not use technology to do anything harmful, illegal, or unethical.
5. I will not share personally identifiable information about myself or others (unless under teacher direction for instructional purposes only).
6. I will not access, post, submit, publish, or display harmful or inappropriate content that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of other based on their race, ethnicity, national origin, sex, gender, sexual orientation, disability, religion or political beliefs. *Harmful matter* includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts, in a patently offensive way, sexual content and which lacks serious literacy, artistic, political, or scientific value for minors (Penal Code 313)
7. I will protect the integrity of technology I use, or that is used by others (District/school equipment, network, programs, and services).
8. I will assist in keeping the Eureka USD network free from viruses, disruption, or other malicious attacks by refraining from opening attachments from unknown sources, downloading and/or installing unauthorized software on District devices, possession and use of malicious software on personal devices (BYOD), and being alert to warnings.
9. If I have been issued an individual Eureka USD network account, I will be the sole user of that account. I will protect my account by not giving out my password and I will report any suspected misuse of my account immediately to the appropriate teacher or administrator.
10. I know the District reserves the right to monitor use of the district's systems for improper use without advance notice or consent. I know that computer files and electronic communications, including email, are not private and may be accessed by the district for the purpose of ensuring proper use. I know that the school reserves the right to inspect a student's personal device if there is reason to believe that the student has violated Board policies, administrative procedures, school rules or has engaged in other misconduct while using the device.
11. I will not manipulate the data or files of other users, or interfere with other users' ability to use technology resources.
12. I will not attempt to bypass security measures, including but not limited to the Internet content filter or by deliberately disguising my identity through the use of anonymizers or proxies.
13. I will report any known misuse of technology or network services to the appropriate teacher, administrator, or the District Office.
14. I will follow all applicable copyright laws. I understand that inappropriately copying or misusing other people's work may be considered plagiarism. Likewise, any work that I create through the use of the Eureka USD technology is my own own property, yet is it subject to all of the guidelines in this policy.
15. I understand that Eureka USD, or its schools, does not assume responsibility for the accuracy or reliability of information obtained through Internet research and access. Developing digital literacy skills is a learning process that requires teacher and parent guidance plus my own responsible use.
16. I will be prepared to be held accountable for my actions (and the loss of privileges and consequences resulting from violations of this agreement).
17. I understand that the school is in no way responsible for repairing or replacing damaged or stolen personal devices or related technology equipment.

Student and Parent/Legal Guardian Acknowledgement for Student-Technology Acceptable Use Agreement

Student Acknowledgment

I have received, read, understand, and agree to abide by this Agreement and other applicable laws and District policies and regulations governing the use of District Technology. I understand that there is no expectation of privacy when using District Technology. I hereby release the District and its personnel from any and all claims and damages arising from my use of District Technology or from the failure of any technology protection measures employed by the District. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name (Please print) _____ Grade: _____

School: _____

Signature: _____ Date: _____

Parent or Legal Guardian Acknowledgment

If the student is under 18 years of age, a parent/guardian must also read and sign the Agreement.

As the parent/guardian of the above-named student, I have read, understand, and agree that my child shall comply with the terms of the Agreement. By signing this Agreement, I give permission for my child to use District Technology and/or to access the school's computer network and the Internet. I understand that, despite the District's best efforts, it is impossible for the school to restrict access to all offensive and controversial materials. I agree to release from liability, indemnify, and hold harmless the school, District, and District personnel against all claims, damages, and costs that may result from my child's use of District Technology or the failure of any technology protection measures used by the District. Further, I accept full responsibility for supervision of my child's use of his/her access account if and when such access is not in the school setting.

Name: (Please print) _____ Date: _____

Signature: _____

*Please detach this page and submit the **Student and Parent/Legal Guardian Acknowledgement for Student-Technology Acceptable Use Agreement** with the **Annual Parent Notice (Authorization Page)** to the school office.*

Purpose: The Eureka Union School District Governing Board intends that technological resources provided by the district be used in a safe, responsible and proper manner in support of the instructional program and for the advancement of student learning.

Terms of the Student Acceptable Use Agreement

Acceptable Use: District students are only permitted to use District Technology for purposes which are safe (pose no risk to students, employees or assets), legal, ethical, do not conflict with the mission of the District, and are compliant with all other District policies. Usage that meets these requirements is deemed "proper" and "acceptable" unless specifically excluded by this policy or other District policies. The District reserves the right to restrict online destinations through software or other means.

Specifically, the student:

- Should use the resources available through the Internet and other electronic media to supplement material available through the classroom, library or through any other resource provided by the school.
- Should adhere to guidelines each time the Internet is used at home and school.
- Should make available for inspection by an administrator or teacher upon request any messages or files sent or received at any Internet location.
- Should use appropriate language in all communications. The student should not use profanity or obscenity and should avoid offensive or inflammatory speech.
- Should abide by copyright laws and should only download/import music or other files to a school-owned computer, including laptop, that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.
- Should use his or her real name in all educational activities that incorporate technology or the Internet (e.g., distance learning, online distance learning, etc.)
- Should respect the privacy of others. The students should re-post (to make appear online again) communications only after obtaining the original author's prior consent.
- Should use technology for school-related purposes only during the instructional day.

Additionally, the District expressly prohibits:

- Participation in "Cyber Bullying" such as attacks and/or threats on/against anyone using these resources. The student should report to responsible school personnel any personal electronically transmitted attacks in any form made by others over the Internet and Local Area Network (LAN) observed while using school-owned technology.
- The use of material (files) or attempt to locate material (files) that are unacceptable in a school setting. This includes, but is not limited to, pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials (files). The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school library. Specifically, all school-owned computers should be free at all time of any pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials (files).
- Accessing or attempting to access instant messages, chat rooms, forums, e-mail, message boards, or host personal web pages, except school-approved, teacher-supervised filtered Internet communication, during the instructional day.
- Attempting to discover password or to control access to the Internet or the computer network.
- Engaging in or attempting to change the configuration of the software that controls access to the Internet or any other electronic media.
- Downloading any programs, files, or games from the Internet or other sources that can be run or launched on the computer as a stand-alone program. These programs of files are sometimes called "executables files."
- Using this resource for any illegal activity. This includes, but is not limited to, tampering with computer hardware or software, unauthorized entry into computers, and vandalism or destruction of computer files.
- Sharing passwords with anyone for any reason and should make every effort to keep all passwords secure and private.
- Playing games, including Internet-based games, except school-approved, teacher-supervised educational games, during the instructional day.
- Bypassing or attempting to bypass the Eureka Union School District's filter software.

Accountability: Users are prohibited from anonymous usage of District Technology. In practice, this means users must sign in with their uniquely assigned District User ID before accessing/ using District Technology. Similarly, "spoofing" or otherwise modifying or obscuring a user's IP Address, or any other user's IP Address, is prohibited. Circumventing user authentication or security of any host, network, or account is also prohibited.

Disclaimer: The District cannot be held accountable for the information that is retrieved via the network. The District will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by the District Systems, System Administrators or your own errors or omissions. Use of any information obtained is at your own risk. The District makes no warranties (expressed or implied) with respect to: (a) the content of any advice or information received by a student, or any costs or charges incurred as a result of seeing or accepting any information; or (b) any costs, liability, or damages caused by the way the student chooses to use his or her access to the network.

Password Policy: Passwords must not be shared with anyone and must be treated as confidential information. Passwords must be changed as often as required by the District's IT department. All Users are responsible for managing their use of District Technology and are accountable for their actions relating to security. Allowing the use of your account by another user is also strictly prohibited. All passwords created for or used on any District Technology are the sole property of the District. The creation or use of a password by a student on District Technology does not create a reasonable expectation of privacy.

Responsibility: Users are responsible for their own use of District Technology and are advised to exercise common sense and follow this Agreement in regards to what constitutes appropriate use of District Technology in the absence of specific guidance.

Revocation of Authorized Possession: The District reserves the right, at any time, for any reason or no reason, to revoke a User's permission to access, use, or possess District Technology.

Restriction of Use: The District reserves the right, at any time, for any reason or no reason, to limit the manner in which a User may use District Technology in addition to the terms and restrictions already contained in this Agreement.

Third-Party Technology: Connecting unauthorized equipment to the District Technology, including the unauthorized installation of any software (including shareware and freeware), is prohibited.

Reporting: If a student becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of District Technology, he/she shall immediately report such information to the Superintendent or designee.

Consequences for Violation: Violations of the law, Board policy, or this Agreement may result in revocation of a student's access to District Technology and/or restriction of his/her use of District Technology and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, Board policy, or this Agreement may be reported to law enforcement agencies as deemed appropriate.

Enforcement

Record of Activity: User activity with District Technology may be logged by System Administrators. Usage may be monitored or researched in the event of suspected improper District Technology usage or policy violations.

Blocked or Restricted Access: User access to specific Internet resources, or categories of Internet resources, deemed inappropriate or non-compliant with this policy may be blocked or restricted. A particular website that is deemed "Acceptable" for use may still be judged a risk to the District (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction.

No Expectation of Privacy: Users have no expectation of privacy regarding their use of District Technology. Log files, audit trails and other data about user activities with District Technology may be used for forensic training or research purposes, or as evidence in a legal or disciplinary matter. Users are on notice that District Technology is subject to search and seizure in order to facilitate maintenance, inspections, updates, upgrades, and audits, all of which necessarily occur both frequently and without notice so that the District can maintain the integrity of District Technology. All data viewed or stored is subject to audit, review, disclosure and discovery. Such data may be subject to disclosure pursuant to the Public Records Act (California Government Code section 6250 et seq.). Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by District Technology for sending or receiving private or confidential electronic communications. System Administrators have access to all email and will monitor messages. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities and/or District personnel.

The District reserves the right to monitor and record all use of District Technology, including, but not limited to, access to the Internet or social media, communications sent or received from District Technology, or other uses within the jurisdiction of the District. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Students should be aware that, in most instances, their use of District Technology (such as web searches or emails) cannot be erased or deleted. The District reserves the right to review any usage and make a case-by-case determination whether the User's duties require access to and/or use of District Technology which may not conform to the terms of this policy.

Specific Consent to Search and Seizure of District Technology: The undersigned consents to the search and seizure of any District Technology in the undersigned's possession by the District, the District's authorized representative, a System Administrator, or any Peace Officer at any time of the day or night and by any means. This consent is unlimited and shall apply to any District Technology that is in the possession of the undersigned, whenever the possession occurs, and regardless of whether the possession is authorized. The undersigned waives any rights that may apply to searches of District Technology under SB 178 as set forth in Penal Code sections 1546 through 1546.4.

Definitions

Blogging
An online journal that is frequently updated and intended for general public consumption.

E-mail
The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical e-mail clients include Microsoft Outlook.

Chain e-mail
E-mail sent to successive people. Typically, the body of the note has directions to the reader to send out multiple copies of the note so that good luck or money will follow.

Flaming
The use of abusive, threatening, intimidating, or overly aggressive language in an Internet communication.

Hacking
Gaining or attempting to gain unauthorized access to any computer systems, or gaining or attempting to gain unauthorized access to District Technology.

District Technology
All technology owned or provided by the District to authorized users, including Internet/Intranet/Extranet-related systems, computer hardware, software, Wi-Fi, electronic devices such as tablet computers, USB drives, cameras, smart phones and cell phones, telephone and data networks (including intranet and Internet access), operating systems, storage media, wireless access points (routers), wearable technology, PDA's, network accounts, web browsing, blogging, social networking, and file transfer protocols, email systems, electronically stored data, websites, web applications or mobile applications, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through District-owned or personally owned equipment or devices.

Instant Messaging
A type of communications service that enables the creation of a kind of private chat room with another individual in order to communicate in real time over the Internet.

Internet Resources
Websites, instant messaging applications, file transfer, file sharing, and any and all other Internet applications and activities using either standard or proprietary network protocols. Examples of websites that pose a risk to the District, or are counter to its mission, are malware repositories, sites advocating violence against civil society or against persons based on race, religion, ethnicity, sex, sexual orientation, color, creed or any other protected categories, sites offering gambling activities or that are pornographic in nature.

IP Address
Unique network address assigned to each computing device connected to a network to allow it to communicate with other devices on the network or Internet.

Malware
Malware is any software, application, program, email or other data or executable code which is designed to cause harm to a network or computer or violate any law, statute, policy or regulation in any way. Examples of harmful activity or intent are theft of personal information or intellectual property by phishing or other means, hacking, violation of copyright law (distributing or copying written material without proper authorization), propagation of Spam e-mails, harassment, extortion, denial of service and facilitating access to illegal content (pornography, gambling, etc.). Accessing or storing malware is expressly prohibited unless authorized for research or forensic purposes by appropriately authorized and designated employees.

Network
Any and all network and telecommunications equipment, whether wired or wireless, controlled or owned by the District which facilitate connecting to the Internet.

Phishing
Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Sensitive information
Classified as Protected Health Information (PHI), Confidential Information or Internal Information.

Spam
Spam is unsolicited nuisance Internet E-mail which sometimes contains malicious attachments or links to websites with harmful or objectionable content.

Spoofing
IP Address spoofing is the act of replacing IP address information in an IP packet with falsified network address information. Each IP packet contains the originating and destination IP addresses. By replacing the true originating IP address with a falsified address a hacker can obscure their network address and hence, the source of a network attack, making traceability of illegal or illegitimate internet activity extremely difficult.

System Administrator
District employees whose responsibilities include District Technology, site, or network administration. System Administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, auditing District Technology, and keeping District Technology operational.

Unauthorized Disclosure
The intentional or unintentional act of revealing restricted information to people, both inside and/or outside the District, who do not have a need to know that information.
User or Users
Individual(s) whether students or employees, full or part-time, active or inactive, including interns, contractors, consultants, vendors, etc. who have used District Technology, with or without the District's permission.

User ID
Uniquely assigned Username or other identifier used by a student to access the District network and systems.