Parent/Student Copy

2018-2019

ESCONDIDO UNION HIGH SCHOOL DISTRICT

Computing Device / Network / On-line Services

Technology Ethical Use Policy

Every student and his/her parent/guardian must complete a TECHNOLOGY ETHICAL USE POLICY CONTRACT before students can use school technology computer systems on campus. Signed forms are turned in during your students' registration appointment and are on file in the Assistant Principal's office during the school year.

ETHICAL USE POLICY and STUDENT / PARENT/GUARDIAN CONTRACT

Before using computer / network / on-line services, the student and parent/guardian shall sign the district's user contract indicating that the student understands and agrees to abide by specified user obligations and responsibilities. Please read this document carefully. When signed/initialed by you and your parent/guardian, it becomes legally binding.

1. **Personal Responsibility:** The student in whose name an account is issued is responsible for its proper use at all times. Users shall maintain privacy of account names/numbers, passwords, and personal information. They shall use the system only under the assigned account.

2. **Digital Literacies:** The EUHSD District recognizes the importance of preparing students for college and careers by providing instruction in digital literacies (keyboarding, Internet search, ethical use/Internet safety, collaboration, and productivity tools). The district creates and manages third-party accounts for students so they can complete a specific class-oriented task/teaching strategy or to complete a class project. Examples include: Office 365, Google Apps for Education and Canvas (an educational collaboration site). Staff and students may also use social media sites such as Facebook and Twitter in educational ways in accordance to the District's School Board social media guidelines (Board Policy 1114)

3. **Acceptable Use:** The use of the account must be in support of education and research and consistent with the educational objectives of the District.
   - Users shall not publish, display, transmit, or receive any material which they know or have reason to know is defamatory, inaccurate, abusive, obscene, profane, sexually oriented, potentially offensive to others, or disrupts the educational process.
   - Neither the school's network nor the broader Internet, whether accessed on campus or off campus, either during or after school hours, may be used for the purpose of harassment often called cyberbullying. All forms of cyberbullying are unacceptable.
   - Use of other organizations' networks or computing resources must comply with the rules appropriate to that network.
   - Transmission, receiving, or downloading of any material in violation of any U.S. or state regulations is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.
   - Use for product advertisement, political lobbying, or partisan political activities, except as an approved part of a course to teach students about the American political system in accordance with District-approved curriculum, is also prohibited.

4. **Privileges:** The use of the information system is a privilege, not a right, and inappropriate use will result in a termination of this privilege. Staff will determine whether a use is inappropriate under this Ethical Use Policy and Contract and the decision is final. The administration has the authority to deny, revoke, or suspend specific user accounts for violation of this Ethical Use Policy and Contract. An administrator may close an account at any time and for any duration as deemed necessary for violation of this Ethical Use Policy and Contract.

5. **Network Etiquette:** You are expected to abide by accepted rules of network etiquette. These rules include (but are not limited to) the following:

- Be polite. Never send or encourage others to send abusive messages.
- Use appropriate language. Never swear; never use vulgarities or any other inappropriate language.
- Do not reveal your or any other person's personal or private information such as: home address, phone number, student ID, or similar information.
- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities must be reported to school authorities, or law enforcement agencies.
- All activities may be monitored. The network is not private; there is no confidentiality, including use of your own device on the school's network.
- Do not use the network in any way that would disrupt the use of the network by others.

6. **Security:** Security on any computer system is a high priority, especially when the system involves many users. If you identify a security problem notify, immediately, the teacher or adult in charge. Never demonstrate the problem to other users. Never use someone else's account and never give out your password to anyone. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network system.

7. **Privacy:** The EUHSD takes student's privacy very seriously. The EUHSD makes every effort to keep personally identifiable information about students private and secure.

8. **Services:** The District will not be responsible for any damages consequential, incidental, or otherwise that you may suffer arising from use of the information system, including damages arising as a result of the negligent or intentional action of the District. This includes loss of data for any reason. Use of any information obtained via the network is at your own risk. Some systems may contain inaccurate, defamatory, abusive, obscene, profane, sexually oriented, or illegal material, and the District does not condone or permit the use of such material in the school environment. The District specifically denies any responsibility for the accuracy or quality of information obtained through the network and on-line services.

9. **Vandalism:** Users, or parents of users who are minors, will be held responsible for damage to hardware and/or software, pursuant to State law. Vandalism includes, but is not limited to, damage to or theft of system hardware or software; the altering of system software; the placing of unlawful information, computer viruses or harmful programs on or through the computer system in either public or private files or messages. **The District reserves the right to remove files, limit or deny access, or to pursue legal remedies for loss sustained, including but not limited to, replacement of hardware and/or software and related labor charges (currently billed at $100.00 per hour), fines, or imprisonment, as applicable.**

10. **Materials:** The District reserves right of access to any material stored in files that are accessible by others and may in accordance with law, remove any material that is obscene, defamatory or otherwise unlawful. Users will not use their account or access privileges to obtain, view, download, or otherwise gain access to such materials.

11. **Account/Password:** The District network system is intended for the exclusive use of its registered users, who are responsible for the use of their account/password. Any problems that arise from the user's account are the responsibility of the account holder. Misuse of the account or use of the account by someone other than the registered holder will be grounds for loss of privilege.

12. **Updating:** The District may occasionally require new registration and account information from you to continue the service. You must notify the teacher or adult in charge of any changes in your account information. Please be aware that the above rules and regulations may change as deemed necessary. The account holder will be informed about subsequent changes.

13. **Discipline:** Students found to be in violation of the computer Ethical Use Policy are subject to school disciplinary measures. Refer to document: "***Technology Infractions***" in the student handbook.

Examples of Technology Infractions

2018-2019 School Year

- Improper use of the network
  - Unauthorized downloading
  - Unauthorized MP3s/streaming audio files
  - Unauthorized streaming movies
  - Downloading/use of Applications unrelated to school
  - Unauthorized IM or “chatting”
  - Peer to peer sharing applications
- Hacking
  - Stealing of passwords
  - Building backdoors
  - Launching DOS attacks
  - Intentional spread of viruses or malware
  - Intentionally bypassing network security devices
  - Attacking external sites
  - Unauthorized access to network equipment
  - Intentionally bypassing network software or hardware configuration
  - Deleting or modifying items or aspects of the network
- Any form of Harassment / Threats / Slander
  - Using district property to view or disseminate inappropriate material (i.e. porn, hate crimes, violent material, etc.)
  - All forms of cyberbullying are unacceptable.
- Use of other student accounts
- Unauthorized and / or unsupervised use of teacher computer station
- Physical Theft / Vandalism
- Attaching unauthorized devices to the network
- Using school computing devices after privileges have been suspended
- Negligence
- Virus or malware distribution
- Distribution of passwords
- Installing unauthorized software

Cyberbullying

Neither the school's network nor the broader Internet, whether accessed on campus or off campus, either during or after school hours, may be used for the purpose of harassment.

All forms of harassment in cyberspace, often called cyberbullying, are unacceptable.

Cyberbullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or Website postings (including blogs). Often the author (sender or poster) of the inappropriate material is disguised (logged on) as someone else.

Community members who feel that they have been the victims of such misuses of technology should not erase the offending material from the system. They should print a copy of the material and immediately report the incident to a school administrator.

All reports of cyberbullying will be investigated fully. Sanctions may include, but are not limited to, the loss of computer privileges, detentions, suspensions, expulsion from school, fines, imprisonment and further legal action.

School copy (return at registration)

Escondido Union High School District
Computer / Network / On-Line Services: Technology Ethical Use Policy Contract
For Student & Parent/Guardian
By signing below: We have read, understand and agree to the
2018-2019 Technology Ethical Use Policy

STUDENT NAME ____________________________________ School ______________________
(Print) Last Name, First Name

Student Signature ____

I.D. Number ________________________ Grade __________ Date ________________

Parent/Guardian Name ____
(Print) Last Name, First Name

Parent/Guardian Signature ____

Parent/Guardian Email: ____

Does your student(s) have reliable access to the Internet to complete school assignments at home? ___YES ___NO

Do you have wireless (WiFi) Internet access at home? ___YES ___NO