Hamilton Unified School District

ACCEPTABLE USE AGREEMENT

Hamilton Unified School District provides a network of computers and computer services to its staff and students. The Internet is a collection of networks that allows access to an unprecedented amount of tools and information. The result is enhanced collaboration, learning, and classroom instruction. We are pleased to be able to provide this level of technology to both staff and students.

With access to such a great wealth of tools and information, both staff and students (collectively referred to as "users") must understand and practice proper ethical use. All users must understand their responsibilities regarding procedures, policy, and security before using the network.

Important General Usage Guidelines:

1. All software installed on any computer must be approved by the district and proof of licensing must be on file at the school site using the software.
2. Only websites that are related to work, instruction, or research are authorized for use.
3. All Games are strictly forbidden from use unless they are educationally related to the curriculum being taught.
4. Streaming video and audio is not authorized unless educationally or instructionally related.
5. All music and file sharing programs (Napster, Morpheus, Kazaa, Gnutella, iMesh, etc.) are banned from use on campus.
6. File storage on campus computer systems is to be used for educational, instructional, or work-related use only. Do not store games, videos, inappropriate pictures, hacking utilities, etc. on any computer or network resource.
7. Any unauthorized access or attempted access to the student records information system will result in strict disciplinary action.
8. The use of any HUSD name on unauthorized web pages, email messages, chat rooms, or message boards is prohibited.
9. No student or staff member shall access inappropriate material via the Internet while on campus and using school resources. This includes, but is not limited to, pornographic sites, child pornography, racist sites, illegal activities, and any other site that is unlawful, immoral, or unethical. This policy includes all technology resources such as computers, phones, VCRs, or TVs.

Users must never share their accounts with other users. Users are responsible for the accounts they have been issued. Therefore, it is extremely important that the password issued to the user be kept confidential to ensure proper network security.

Users are restricted from downloading, storing, or using any program designed to exploit network vulnerabilities. Copyrighted material such as music, pictures, media files, and programs shall not be downloaded or stored on any campus computer without proof of purchase or written consent from the owner. Any user identified as intentionally sending or infecting computers with a Virus or Trojan will be subject to disciplinary action and/or legal action. All users must understand the network and computers are the property of the school district, which can and will be monitored for content and usage.

Internet:

1. The Hamilton Unified School District (HUSD) has actively pursued advanced technology to provide access to learning opportunities for our students and staff. We believe this computer technology will help propel today's schools into the information age by allowing students and staff to access and use information sources from distant computers, communicate and share information with individuals or groups of other students and staff, and significantly expand their knowledge base. The Internet is a tool for lifelong learning that will open the door to many advanced educational tools.

Proper and Ethical Use:

1. Students and staff must understand and practice proper and ethical use.

Penalties for Improper Use:

1. Any user violating these rules, applicable state and federal laws or posted classroom and district rules are subject to loss of network privileges and any other District Disciplinary options.
2. In addition, pursuant to the State of California Law, any unauthorized access, attempted access, or use of any state computing and/or network system is a violation of section 502 of the California Penal Code and/or other applicable federal laws, and is subject to criminal prosecution.

Acceptable Use:

1. The purpose of the Internet is to facilitate communications in support of research and education, by providing access to unique resources and an opportunity for collaborative work. To remain eligible as a user, the use of your account must be in support of and consistent with the educational objectives of HUSD. HUSD users of the Internet must comply with existing rules and acceptable use policies, which are incorporated into this document, and are available from HUSD.
2. Transmission of any material in violation of any United States or state regulation is prohibited. This includes, but is not limited to, copyrighting material, threatening or obscene material, or material protected by trade secret.
3. Use for commercial activities is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

Privilege:

1. The use of the Internet is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege. Under this agreement, HUSD is delegated the authority to determine appropriate use and may deny, revoke, suspend or close any user account, at any time, based upon its determination of inappropriate use by the account holder or user.

Monitoring:

1. HUSD reserves the right to review any material on user accounts, computers, and file server space in order to make determinations on whether specific uses of the network are inappropriate. In reviewing and monitoring user accounts and file server space, HUSD shall respect the privacy of those accounts.

Network Etiquette:

1. Be polite. Do not use abusive language in your messages to others.
2. Use appropriate language. Do not use profanities, vulgarities, or any other inappropriate language. Do not engage in activities that are prohibited under state or federal law.
3. Do not reveal any personal information about yourself, students, or colleagues. This includes personal addresses and phone numbers.
4. Note that electronic mail (email) is not guaranteed to be private. People who operate the system do have access to all email. Messages relating to or in support of illegal activities may be reported to the authorities and may result in the loss of user privileges.
5. Do not use the network in such a way that you would disrupt the use of the network by other users.
6. All communications and information accessible via the network is assumed to be private property.

No Warranties:

1. HUSD makes no warranties of any kind, whether expressed or implied for the services it provides. HUSD will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, incorrect deliveries, or service interruptions caused by HUSD's negligence or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. HUSD specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they contain and consider how valid that information may be.

Security:

1. Security on any computer system is a high priority, especially when the system involves many users. Users must never allow others to use their password. Users should also protect their password to ensure system security and their own privilege and ability to continue to use the system.

2. If you feel that you have identified a security problem on the network, you must notify a system administrator. Do not demonstrate the problem to other users.
3. Do not use another individual's account without express written permission of the account holder.
4. Attempts to log on to the network as a system administrator may result in cancellation of user privileges.
5. Any user attempting to operate a malicious piece of software designed to hack, crack, or alter any part of the network, elevate user privileges, or produce unnecessary bandwidth consumption will have disciplinary action taken against them.
6. HUSD may deny Internet access to any user identified as a security risk for having a history of problems with other computer systems.

Vandalism and Harassment:

1. Vandalism and harassment will result in cancellation of user privileges.
2. Vandalism is defined as any malicious attempt to harm, modify, and destroy data of another user, the Internet or other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creating of computer viruses, Trojans, and other malicious software.
3. Harassment is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted email.

Procedures for Use:

1. Student users must always get permission from their instructors before using the network or accessing any specific file or application.
2. All users have the same right to use the equipment. Therefore, users shall not play games (network or local) or use the computer resources for other non-academic activities. All users agree to talk softly and work in ways that will not disturb other users.

Encounter of Controversial Material:

1. Although the district employs an Internet Filtering Device, users may encounter material that is controversial and which users, parents, teachers or administrators may consider inappropriate or offensive. However, on a global network it is impossible to control effectively the content of data and an industrious user may discover controversial material. It is the user's responsibility not to initiate access to such material.

Standards of Use for District Technology (i.e. laptops, etc.)
User Responsibilities:

- Keep the device(s) in a secure location when it is not at school.
- Do not leave the device(s) unattended.
- Adhere to the " Acceptable Use Agreement" at all times.
- Do not alter the device(s) in any way.
- Never loan out your device(s) to other individuals.
- Charge your device(s) battery daily.
- Do no remove any serial numbers, barcodes or other identifying labels from the device(s).
- Protect the device(s) from damage from food, liquids or other harmful materials and from extremes of heat and cold.
- Do not disassemble any part of your device(s) or attempt any repairs.
- Only use your device(s) in ways that are appropriate and educational.
- Do not place decorations (such as stickers, markers, etc.) on the HUSD device(s).
- Understand that your device(s) is subject to inspection at any time without notice.
- Be responsible for all damage or loss caused by neglect or abuse.
- Agree to "Damage Fees of District Owned Technology or Accessories" listed below.
- Agree to return the device(s) and power cords in good working condition.

Damage Fees of District Owned Technology or Accessories:

Tier	Fee
First Offense: District will pay for the repair or replacement depending on the situation. *Egregious offenses can be moved to the third tier.* • Full Laptop Replacement • Charger • Screen • Keyboard • Other Damage as assessed (scratches, abrasions, vandalism, etc.) • Copy Card	**First Offense Fees:** No fee as the District will cover the repair or replacement of the Device or it's accessories. • $0 for each item listed
Second Offense: District will pay for half of the repair or replacement depending on the situation. Egregious offenses can be moved to the third tier. • Full Laptop Replacement • Charger • Screen • Keyboard • Other Damage as assessed (scratches, abrasions, vandalism, etc.) • Copy Card	**Second Offense Fees:** District will cover half the cost of the repair. The employee will be responsible for the remaining cost. • TBD depending on cost of laptop • $50 • $150 • $75 • TBD depending on damage • $7.50
Third Offense: Employee will cover the full cost of repair or replacement. • Full Laptop Replacement • Charger • Screen • Keyboard • Other Damage as assessed (scratches, abrasions, vandalism, etc.) • Copy Card	**Third Offense Fees:** Employee will cover the full cost of repair or replacement. • TBD depending on cost of laptop • $100 • $300 • $150 • TBD depending on damage • $15

User:

1. I understand and will abide by the above Conditions, Rules, and Acceptable Use Agreement. I further understand that any violation of the above Conditions, Rules, and Acceptable Use Agreement is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked; disciplinary action may be taken and/or appropriate legal action.
2. I have read the Internet Use Agreement. I understand that this access is designed for educational purposes only. I also recognize that it is impossible for HUSD to restrict access to controversial materials, and I will not hold them responsible for materials acquired on the network. I hereby give permission to issue an account for myself and certify that the information contained on this form is correct.
3. I acknowledge receipt of district property (as applicable) for business use only. I am expected to exercise due care in my use of this property and to utilize such property only for authorized purposes. I do not assume ownership. I understand that the property must be returned at the time of my separation from employment or when it is requested by my manager or supervisor.

Signing below indicates that you, the User, admit to having read, understood, and agree to abide by all provisions and restrictions set forth in this agreement and the attached Board Policy 4040 Employee Use of Technology.

_____

_____	_____	_____
Name of User (please print)	Signature of User	Date

SUBMIT FORM

Hamilton USD
Board Policy – Employee Use of Technology: BP 4040

The Governing Board recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting district and school operations; and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use district technology primarily for purposes related to their employment.

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, 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.

The Superintendent or designee shall establish an Acceptable Use Agreement which outlines employee obligations and responsibilities related to the use of district technology. Upon employment and whenever significant changes are made to the district's Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

Employees shall not use district technology to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

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 or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 6777; 47 USC 254)

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any equipment or other technological resources provided by or maintained by the district, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. To ensure proper use, the Superintendent or designee may monitor employee usage of district technology at any time without advance notice or consent and for any reason allowed by law.

In addition, employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct district business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of district technology to the Superintendent or designee. Inappropriate use of district technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.
Original Adopted Date: 02/22/2017 | Last Reviewed Date: 02/22/2017