Technology Acceptable Use Policy
Policy EEF

Kane School District
Adopted 9-3-2009

1. Purpose

The purpose of this policy is to ensure appropriate, responsible, ethical and legal access and use of computers, the Internet, and other electronic or communication devices by District students, patrons, and employees. The Technology Acceptable Use Policy addresses two distinct concepts of technology use. The first regards the use of computers and the Internet, and the second addresses interfering and electronic communication devices.

2. Policy

2.1. Computers and the Internet

It is the policy of the Kane School District to permit students, patrons, and employees to have computer and Internet access under approved regulations and guidelines, to include those listed in the Children's Internet Protection Act, State Law, and policies adopted by Board (of Education). In general, the user's responsibilities require responsible, decent, ethical, polite, efficient, and legal use of computer and network resources. Students, patrons, and employees must not access obscene, pornographic, or material that is deemed to be harmful to minors. District and school personnel will instruct students and staff on acceptable use of computers and Internet resources and proper network etiquette. All students, patrons, and employees are granted access to the Internet, but all access to the Internet through district resources is subject to the terms of the Technology Acceptable Use Agreement and District policy. All students and school employees must sign an Acceptable Use Policy each year. Schools will keep copies of these signed documents in their files and will provide the District with a spreadsheet showing the signature status of all students and faculty members.

2.2. Interfering and electronic communication devices

While in some instances the possession and use of electronic communication devices or other devices or objects by a student at a school may be appropriate, often the possession and use of such devices or objects by students at school can have the effect of distracting, disrupting, and intimidating others in the school setting and leading to opportunities for academic dishonesty and other disruptions of the educational process. The purpose of this component of the policy is to vest with school administrators the authority to enforce reasonable rules relating to student use of such objects or devices in the public schools.

3. Procedure

3.1. Definitions:

3.1.1. **Acceptable Use**: Computer and Internet use must be consistent with the education objectives of the District. The use must also be consistent with the terms of this policy and all policies adopted by the District.

3.1.2. **Prohibited Use**: Any use that violates federal or State laws and/or District policy.

3.1.3. **Interfering Devic**e: This includes any device or object which does not constitute a weapon or explosive but may, if used or engaged, interfere with the educational process for either the student possessing or using the object or for other students. By example,

such objects include any electronic communication device (defined below), a camera, lasers, laser pens or pointers, radios, portable CD players, or other electronic equipment or devices.

3.1.4. **Electronic communication devic**e: This includes laptop and hand-held computers, telephones, “smart phones”, camera telephones, two-way radios or video broadcasting devices, pagers, and any other device that allows a person to record and/or transmit on either a real time or delayed basis, sound, video or still images, text, or other information.

3.1.5. **Camera:** This includes any device for taking still or motion pictures, whether in a digital or other format.

3.2. Prohibited Uses: The following uses of the District's computers, including its network and Internet access are prohibited including:

3.2.1. using an account other than your own and any attempt to gain unauthorized access to accounts on the network.

3.2.2. attempting to obtain access to restricted sites, servers, files, databases, etc., or attempting to gain unauthorized access to other systems (e.g. "hacking").

3.2.3. student use of games, Internet games, chat rooms, blogs, social networking sites, and instant messaging not specifically assigned or authorized for use by the district. Employees and patrons must not use games, Internet games, chat rooms, blogs, social networking sites, and instant messaging that is not directly related to curriculum development, instruction, or work assignment. If such sites are blocked, access can be requested for appropriate, core-aligned uses on a temporary basis.

3.2.4. using computers, the Internet or network for any illegal activity. This includes, but is not limited to: copyrighted material, threatening or obscene material or material protected by trade secrets. This prohibition includes the violation of any federal, State or local law.

3.2.5. providing personal addresses, phone numbers, and other private information whether that information belongs to the user or any other individual unless it is related to the core curriculum or specifically authorized for release. Additionally, all employees are subject to and must comply with State and federal privacy laws and regulations. The unauthorized disclosure of private or protected information may result in disciplinary action and referral for criminal prosecution.

3.2.6. using the Internet for commercial purposes, financial gain, personal business, product advertisement, use for religious or political lobbying, including student body elections students or representation elections for employees.

3.2.7. attempting vandalism defined as any attempt to harm or destroy data of another user, another agency or network that is connected to the Internet. Vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses. It also includes attempts to gain unauthorized access to a network that is connected to the Internet.

3.2.8. degrading or disrupting network equipment, software, or system performance.

3.2.9. wasting finite network resources.

3.2.10. invading the privacy of individuals or disclosing confidential information about other individuals.

3.2.11. posting personal communications without the original author's consent.

3.2.12. posting anonymous messages.

3.2.13. accessing, downloading, storing or printing files or messages that are profane, obscene, or that use language that offends or tends to degrade others.

3.2.14. harassing others and using abusive or obscene language on the network. The network may not be used to harass, annoy, or otherwise offend other people.

3.2.15. using material which may be deemed to violate any District policy or student code of conduct.

3.2.16. downloading music or video files or any other files that will infringe on copyright laws or is not directly related to a school or position assignment.

3.2.17. communicating threats of violence.

3.2.18. using the network for plagiarism. Plagiarism is taking ideas or writing from another person and offering them as your word. Credit must always be given to the person who created the information or idea.

3.2.19. bypassing district filters and security via proxy servers, VPN access, or other means.

3.2.20. unauthorized purchasing of goods or services online. The District is not responsible for any such purchases.

3.2.21. using VoIP (Voice over IP) software or devices.

3.2.22. installation and use of personal wireless access points. All wireless network access (if any) will be provided by the District.

3.2.23. applying, changing or attempting to change any settings on any computer or computer system belonging to the District without permission

3.2.24. storing any file or information on any school or District server without specific rights granted by the District.

3.3. Privileges and Discipline:

Internet use is a privilege, not a right, and inappropriate use will result in a loss of network privileges, disciplinary action, and/or referral to legal authorities. The system administrators will close an account when necessary. An administrator or faculty member may request the system administrator to deny, revoke, or suspend specific user access and/or user accounts as indicated:

Minor Violations:

1. Loss of computer privileges or Internet access rights.
    A. First offense: verbal warning and/or loss of Internet access for up to one week as directed by principal.
    B. Subsequent offense for same violation: loss of Internet privilege for a period exceeding one week as directed by principal.

More serious violations:

1. Suspension of Internet or network access for any period exceeding one month;
2. Revocation of Internet or network access;

3. Referral to legal authorities;
4. Suspension from school;
5. Loss of employment if staff or faculty member;
6. Referral to State Professional Practices Board if staff or faculty member.

Authorized District employees have the right to intercept or read a user's e-mail, to review any material, and to edit or remove any material that they believe may be unlawful, obscene, defamatory, abusive or otherwise objectionable. If the District intends to impose any discipline upon a student other than revoking privileges for the remainder of the school year, the student will be afforded appropriate or adequate due process. Career and Provisional Employees will be disciplined according to District Policy. Temporary employees or other patrons may be denied computer access or have their employment terminated.

3.4. Privacy Information:

Nothing is private on the District-owned network. If a user accesses a particular site on the Internet, it is likely that someone knows the connections that the user is making, knows about the computer the user is using and what the user looked at while on the system. Frequently these sites maintain records that can be subpoenaed to identify what the user has been viewing and downloading on the Internet. In addition, the District reserves the right to monitor whatever a user does on the network and to make sure the network functions properly. A user has no expectation of privacy as to his or her communications or the uses made of the Internet.

3.5. Network Etiquette:

Users are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

- be polite.
- do not be abusive in your messages to others.
- use appropriate language.
- do not swear, use vulgarities or any other language inappropriate in a school setting.

3.6. Security:

3.6.1. Security is a high priority on computer networks. If a security problem is identified, the user must notify the system administrator immediately. Do not demonstrate the problem to other users. Users may not use the Internet to discuss or disseminate information regarding security problems or how to gain unauthorized access to sites, servers, files, etc.

3.6.2. Any passwords issued to users/parents/guardians must not be shared with or disclosed to other users without specific authorization from the administrator. Passwords should be changed frequently. (see passwords guidelines document) If students/parents divulge passwords to anyone not authorized by school policy, the school/district cannot guarantee the protection of confidential student information.

3.6.3. Do not leave a workstation without logging out of the network or "locking down" the workstation.

3.6.4. You must report any of the following to a building administrator:

- if you receive or obtain information to which you are not entitled or which is not authorized by this policy;
- if you know of any inappropriate use of the network by others; and
- if you believe the filtering software is not filtering a site or sites that should be filtered under this agreement.

3.7. Disclaimer:

3.7.1. The District makes no guarantee of the completeness or accuracy of any information provided on the network. It makes no promise or warranty to maintain or update its network or the information contained or made available to the public, its employees, and students. The District may suspend or discontinue these services at anytime. The user assumes the risk of verifying any materials used or relied on.

3.7.2. The District disclaims any express or implied warranty in providing its computer system, provided services and any materials, information, graphics, or processes contained therein. It makes no warranty, express or implied, nor assumes any responsibility regarding the use of its network or its contents for its accuracy, completeness, currency, its use of any general or particular purpose, or that such items or use of such items would not violate or infringe on the rights of others. Access to its network is provided on a strictly "as is basis."

3.7.3. The District's network resources may contain hypertext or other links to Internet or computer sites not owned or controlled by the District that may be of interest. The District cannot supervise or control the content of these other sites. Any information, endorsements of products or services, materials or personal opinions appearing on such external sites are not controlled, sponsored or approved by the District.

3.7.4. The District specifically disavows legal responsibility for what a user may find on another external site or for personal opinions of individuals posted on any site, whether or not operated by the District.

3.7.5. A user assumes the risk of use or reliance on any information obtained through the network.

3.7.6. The District will not be responsible for any damages a user suffers while on the system, including loss of data resulting from delays, non-deliveries, misdeliveries or service interruptions caused by negligence, errors, or omissions.

3.8. Access and/or Accounts Requirements

All users are responsible for reading and agreeing to follow all guidelines outlined in the Acceptable Use Policy (AUP). Employees may be granted an account for their term of employment subject to the terms, limitations, and conditions outlined in this policy.

3.9. Summary of Interfering and Communication Devices - See District Policy FGAH -

Except as set forth below, a student may possess, but may not operate or engage, any interfering device during school hours or at school functions, unless specifically authorized in advance by the school personnel in charge of the class or activity.

3.9.1. It is District policy that students and others in the District will not be subject to video or audio capture, recording or transmission of their words or images by any student at a school without express prior notice and explicit consent for the capture, recording or transmission of such words or images.

3.9.2. During any time when a student is scheduled to be in class or involved in a regular school activity, it is a violation of policy for the student to have in his or her possession an electronic communication device or camera which is in the "on" position and ready to receive, send, capture, or record any communication, visual image, sound, text message or other information.

3.9.3. Electronic communication devices and cameras must not be possessed, activated, or utilized at any time by any person, to include a student, teacher, staff employee, patron, or any other individual, in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower rooms, restrooms, and any other areas where students or others may change or be in any stage or degree of disrobing or changing clothes.

3.9.4. The principal or administrator of the school is hereby given authority to make determinations as to other specific locations and situations where possession of electronic communication devices and cameras is absolutely prohibited.

3.9.5. At no time may any electronic communication device or camera be utilized by any student in any way which gives the impression to others of being threatened, humiliated, harassed, embarrassed, or intimidated.

3.10. Sanctions Confiscation of Device

Any electronic device found on District property is subject to search and confiscation. Pornographic or indecent material will be reported for possible criminal prosecution in accordance with the UCA 76-10-1235 and/or other applicable District, state and federal regulations. For each observed violation of this policy, it shall be the duty of the school staff, teacher or administrator observing the violation to immediately confiscate the interfering device. Employee or patron violations will be immediately reported to the appropriate school or District administrator. Furthermore, the school or District may take additional disciplinary action as described in other District policies. The confiscated device shall be forwarded to the administrative office together with the name of the person from whom the device was confiscated and the reason for the confiscation. The school office should make arrangements to notify the parent/guardian of the student from whom the device was confiscated and arrange for the parent or guardian to pick up that device at the school office.

3.11. Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and District policies. See District Policy FGAH.

Computer Anti-Virus Guidelines

1. Purpose

This policy establishes standards and best practices that must be met when any computer or computing device, both wired and wireless, is connected to Kane School District networks to prevent obtaining and spreading computer viruses. These are basic steps that all users must take to ensure that Kane School District computers and networks remain stable and available at all times.

2. Scope

This policy covers all users of computers running any sort of user installable and configurable operating systems (Windows, Mac OS, Linux, etc.) that are used in the District or are connected to the District network either through a wired Ethernet connection or by wireless networking.

3. Policy

3.1 Expectations

3.1.1 Users are expected to use district installed and approved software applications.

3.1.2 Users are not authorized to install unlicensed software on computers. If a user requires special or non-standard software to be installed on computers for District use, it must be cleared by District Technology administration. The user will be responsible for supplying licenses, media, and any documentation. License information is a requirement of the District Auditors.

3.1.3 Users are ultimately responsible for their own data. Users must back up critical data and system configurations on a regular basis and store the data in a safe place.

3.1.4 Users must run the District standard, supported anti-virus software that is available from the District Technology Coordinator or his designees. Users must run the current version and download and install anti-virus software updates as they become available.

3.2 Best Practices

3.2.1 Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

3.2.2 Delete spam, chain, and other junk email without forwarding, in accordance with the Districts Acceptable Use Policy.

3.2.3 Never download files from unknown or suspicious sources.

3.2.4 Avoid direct disk sharing with read/write access unless there is absolutely a District requirement to do so.

3.2.5 Always scan a floppy diskette or any portable storage device from an unknown source for viruses before using it.

3.2.6 New viruses are discovered almost every day. Periodically check the Anti-Virus for updates and download and install any available updates.

3.2.7 Always use the current & up to date version of any software application on your computer. The District will not attempt to make old or outdated software work with newer installed operating systems.

3.3 Results of Non-Compliance

3.3.1 Any non-approved software installations will not be supported.

3.3.2 Any machine that is found to have software installed that has not been approved by the district or does not have a current and active license will be reformatted and all data will be wiped clean.

3.3.3 Any machine that has been infected by a virus that can not be removed from a Users computer will be formatted and wiped clean of all data. The District will reinstall the appropriate system operating software and District approved software only. Any user data on the machine may/will be lost.

Wireless Security Guidelines

1. Purpose

This policy establishes standards that must be met when wireless communications equipment is connected to Kane School District networks. The policy prohibits access to Kane School District networks

via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Security are approved for connectivity to Kane School District's networks.

2. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, Bluetooth equipped devices, and 802.15 devices etc.) connected to any of Kane School District's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Kane School District's networks do not fall under the purview of this policy.

3. Policy

3.1 Approved equipment

All wireless LAN access must use district-approved products and security configurations. All network equipment, both wired and wireless, must be purchased & installed by District technology personnel.

3.2 Monitoring of uncontrolled wireless devices

All District locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved (rogue) wireless access points. All District locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect the presence of wireless devices forming a connection between the network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks or computers participating in ad-hoc or peer-to-peer wireless networking. In District locations where wireless LAN access has been deployed, whenever possible, wireless intrusion detection systems will be deployed to monitor for attacks against the wireless network.

3.3 Authentication of wireless clients

All access to wireless networks must be authenticated. The District's existing password policy must be followed for access to wireless networks. The strongest form of wireless authentication permitted by the client device must be used. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network. Any District user with an account in a District user database shall be able to authenticate at any District location where wireless access is present.

3.4 Encryption

All wireless communication between District devices and District networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement. The strongest form of wireless encryption permitted by the client device must be used. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

3.5 Access control policies

- Access to District network resources through wireless networks should be restricted based on the role of the user.
- Unnecessary protocols should be blocked, as should access to portions of the network with which the user has no need to communicate.
- Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security." The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
- Access control rules must use stateful packet inspection as the underlying technology.

3.6 Remote wireless access
Telecommuting employees working from remote locations must be provided with the same wireless standards supported in District offices. Employees should be discouraged from connecting District computers though consumer type wireless equipment while at home in lieu of District-provided equipment. Remote users outside of the district network must connect to district resources using a secure connection such as a VPN.

3.6 Client security standards

- All wireless clients must run District approved anti-virus software that has been updated and maintained in accordance with the District's anti-virus software policy.
- All wireless clients must run host-based firewall software in accordance with the District's host security policy.
- All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the District's host security policy.
- All wireless clients must be installed with District-standard wireless driver software. Clients not conforming with minimum security standards will be placed into a quarantine condition and automatically remediated. Client operating systems that do not support client integrity checking will be given restricted access to the network according to district requirements.

3.7 Wireless guest access

- Wireless guest access will be available at all facilities where wireless access has been deployed.
- All wireless guest access will be authenticated through a web-based authentication system (captured portal) where possible.
- A single username/password combination will be assigned for all guest access. The password for guest access will be changed monthly and distributed to local facility managers. Special accounts may be created for guests on a request basis. Access must be arranged at least 24 hours before planned access.
- Wireless guest access is available from the hours of ____ until ____ .
- Wireless guest access is bandwidth limited to __Mb/s per user.
- Guest access will be restricted to the following network protocols:
    - HTTP (TCP port 80)
    - HTTPS (TCP port 443)
    - IKE (UDP port 500)
    - IPSEC ESP (IP protocol UDP 50)
    - PPTP (TCP port 1723)
    - GRE (IP protocol 47)
    - DHCP (UDP ports 67-68)
    - DNS (UDP port 53)
    - ICMP (IP protocol 1)

Publishing on the Internet Guidelines

1. Purpose:

District and school websites provide instructional resources; information about curriculum, instruction and school authorized activities; and general information relating to our schools and our District's mission. Communication with parents, family, the community and students is important for the District and each classroom teacher. Events and projects can be displayed to show what has been happening in the classroom along with keeping all informed about future events and assignments. It is important that teachers give their web page address to students and parents as often as possible and keep their site updated.

Kane School District teachers will be allowed to create and post their own web pages to the Internet. This will place the primary responsibility for the content of the teacher's page on the teacher. Building administrators, teachers, and the Kane School District are responsible under federal law for the content of these pages. Teachers should be extremely careful whatever they post. It is the responsibility of the teacher, the building administrators and the District to ensure that all District and school hosted web pages follow District policies and state and federal laws. This guide is intended to assist District personnel and teachers in the development and posting of web pages.

2. Policy:

2.1. Teachers posting web pages on District sponsored web servers must adhere to the established rules and guidelines.

2.2. Posting of student work on District sponsored web servers must be in compliance with the established rules and guidelines.

3. Procedure:

3.1. Web Page Rules and Guidelines

3.1.1. This policy provides the basic overview for teachers posting web pages linked to the District webpage. Among the key points are:

3.1.1.1. Teachers and administrators are encouraged to develop links to third party hosts. The links should conform to the "three-click rule" (a visitor should never have to visit more than three pages after the home page to find the information he/she wants.) so that the link does not provide connection to inappropriate sites.

3.1.1.2. Teachers and administrators need to attend training sessions if they are going to create and maintain a web site.

3.1.1.3. The District encourages teachers to involve students in the development of web sites. (Involvement needs to be grade appropriate. Students can be involved in various aspects including layout, design, choosing colors, and offering suggestions).

3.1.1.4. All web pages are subject to evaluation at any time by District administrators.

3.1.1.5. School administrators are responsible for evaluating the content on the school's website, its teacher's pages, and any links off of these pages.

3.1.2. The content and links within the District, school, or teacher web site should:

3.1.2.1. be informative.

3.1.2.2. be accurate.

3.1.2.3. be current.

3.1.2.4. pertain to education or to the functions of the school.

3.1.2.5. be correctly written, spelled and punctuated.

3.1.2.6. be thoughtfully and attractively presented.

3.1.2.7. notify parents/guardians of intent to display a student's name or picture. Although student names and photos are considered "directory information," written parental

permission might be obtained because of the potential worldwide dissemination and loss of control of this information.

3.1.2.8. do not attach a specific phone number or address to any student's name and specific picture,.

3.1.2.9. notify staff members or School Board members of intent to display the name or picture of any staff member or School Board member.

3.1.2.10. require written permission be obtained for single, specific pictures or notify parents of intent to use unless requested otherwise.

3.1.2.11. allow adults to be identified by attaching his/her name to a specific picture.

3.1.3. Content and links (defined as any site that can be reached in two clicks or less) within the District web site or, a teacher/student page linked from the District site, should NOT:

3.1.3.1. contain or point to pornographic, violent, obscene, objectionable or offensive material.

3.1.3.2. violate copyright laws by containing unauthorized or plagiarized content including but not limited to written materials, pictures, graphics, audio, and video.

3.1.3.3. contain any personal information on students without written parental permission.

3.1.4. In order to protect individual privacy and promote good community relations, District web sites or, teacher/student pages linked from the District website, should:

3.1.4.1. never provide addresses, phone numbers or other private information about students.

3.1.4.2. never provide e-mail addresses except for the purpose of supporting or providing feedback for a school-related activity, organization or web site.

3.1.4.3. never contain information or material that the District would not be willing to publish in other media forms (e.g., newspaper, television, brochures, etc.).

3.1.4.4. never allow students to post their personal web pages. If students need to post a web page as part of integrating the classroom curriculum with the Internet, it should be posted on the District web page with teacher approval through the District web master. All links from a student project web page must be checked for appropriateness.

3.1.4.5. never promote specific political, metaphysical or religious viewpoints or agendas. Links to such pages may be placed on a web page for research purposes if the links are balanced.

Laptop use

Notebook/Laptop computers purchased for use in the district need to follow the district guidelines by staying with Windows OS platform. Laptop labs present unique problems, both with security as well as with custody. The primary purpose of notebook labs purchased with HB160 funds is for on-line testing. Every effort must be made to make sure these units are, and continue to be, functional for CBT testing. Any other use of these computers is secondary but it is expected they be used from time to time for student use. Notebook computers are not to be checked out of school to students or teachers. Personal laptop computers are prohibited from Kane School District's regular networks. Kane School District has a "guest wireless" system which is available to everyone for general Internet access requirements. If

students or teachers bring personal laptops to school they must ONLY be connected to the Kane_guest network. No other wireless routers are allowed in the schools other than the Cisco Access Points. Security becomes a major issue with wireless technology. Therefore, student use of laptops must be monitored more closely and in strict accordance with the district Acceptable Use Policy. It becomes the responsibility of the building administrator to insure that the computers are cared for appropriately and that use of the laptops is monitored accordingly.

If teachers check out a laptop lab, they are responsible for care and monitoring of the computer use. Laptop labs that are not cared for and monitored properly will be returned to the district for storage and check-out to schools for on-line testing purposes only. All laptops need to have virus protection installed and active to prevent acquiring or unknowingly transporting viruses to the district network. CDs should not be left in laptops when transporting them. All district-owned laptops are for school use, and should be treated as such. Students are not to save files on the laptops. Encourage users to save personal files to USB flash drives. The laptops may not have floppy drives, but if they do, files may be saved on floppies or files can be saved to the student's gmail account. (Google Docs)

Great care must be taken when transporting laptops. Laptop screens must never have any force applied directly on them. Laptop AC adapters usually wear out or are broken easily if they are not handled with care. Laptop batteries should be stored fully charged. Care must be taken to protect all programs on laptops. To this end, laptops for student use will have Deepfreeze installed on them and may have password protection.

The purchase of laptops for teachers is reserved for the mobile employees in the district. The school principal and the district technology department will determine the need for laptops in a school. Teachers are to treat district purchased notebooks as district property and not as personal property. Laptop computers that have been purchased for specific use and are no longer used for that purpose are to be returned to the district department head for re-distribution as needed. e.g. heating system, door keys, clocks, speech, reading.

Software

Only licensed software may be installed onto District laptops.

Teachers are not authorized to install unlicensed software on computers. If a teacher requires special or non-standard software to be installed on laptops for District use, it must be cleared by District Technology administration. The teacher will be responsible for supplying licenses, media, and any documentation. Breach of these conditions may lead to disciplinary action.

1. For network connection of laptops, users are provided with a secure connection account. The user is to use no other account on the network. The user should at all times keep any passwords for this account secure and private. The user takes full responsibility for the use or misuse of this account.
2. This account allows the user certain privileges and rights on the network. The user should in no way attempt to gain other privileges or to attempt to access resources on the network to which no explicit rights have been granted.
3. The user shall not in any way, tamper or misuse District equipment, either software or hardware. No form of tampering is acceptable.
4. Laptops can have access to the Internet. Abuse of this access, in the form of access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious breach of the law (Child Trafficking and Pornography Act 1998). The District will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.
5. E-mail, where these related to their schoolwork or study, should be used in a courteous manner, respecting the etiquette of the network. Usage of any form of profanity in these communications is absolutely forbidden.
6. Users may not download copyrighted software, any audio or video files, or any copyrighted material from the Internet. Any such material found will be deleted without prior notification.

7. Software in use in the District is licensed in a correct and legal manner. However (except where explicitly stated), it is not available to users for home usage. Users should make no attempt to copy licensed or copyrighted material from the District network or media.
8. District owned computers, either notebooks or desktops, must have district owned antivirus software.
9. The contents of all mailboxes, PCs, server shares and caches operated by the District, remain the property of the District. The status of these data stores is similar to that of letters posted to the District to a post holder (not marked as personal and private).
10. E-Mail should be considered as an insecure medium for the transmission of confidential information. Where confidential information is to be transferred, in particular externally, it should be done in an encrypted form.
11. Notwithstanding that every effort is made to ensure that home folders and e-mail are secure, the District does not in any way guarantee the security of this data.
12. Food and drinks should be kept well away from laptops. The user should also take care when shutting down and closing the lid of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case the user will be liable for repair costs.

Guidelines for User Responsibilities:
Use of Kane County School District Technology resources is granted based on acceptance of the following specific responsibilities:

Use only those computing and information technology resources for which you have authorization.
For example: it is a violation

- to use resources you have not been specifically authorized to use
- to use someone else's account and password or share your account and password with someone else
- to access files, data or processes without authorization
- to purposely look for or exploit security flaws to gain system or data access

Use computing and information technology resources only for their intended purpose.
For example: it is a violation

- to send forged email
- to misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with
- other systems or users
- to use electronic resources for harassment or stalking other individuals
- to send bomb threats or "hoax messages"
- to send chain letters
- to intercept or monitor any network communications not intended for you
- to use computing or network resources for advertising or other commercial purposes
- to attempt to circumvent security mechanisms

Protect the access and integrity of computing and information technology resources.
For example: it is a violation

- to release a virus or worm that damages or harms a system or network
- to prevent others from accessing an authorized service
- to send email bombs that may cause problems and disrupt service for other users
- to attempt to deliberately degrade performance or deny service
- to corrupt or misuse information
- to alter or destroy information without authorization

Abide by applicable laws and universal policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
For example: it is a violation

- to make more copies of licensed software than the license allows
- to download, use or distribute pirated software
- to operate or participate in pyramid schemes
- to distribute pornography to minors
- to upload, download, distribute or possess child pornography

Respect the privacy and personal rights of others.
For example: it is a violation

- to tap a phone line or run a network sniffer without authorization
- to access or attempt to access another individual's password or data without explicit authorization
- to access or copy another user's electronic mail, data, programs, or other files without permission

KCSD Laptop Use and Security Agreement
As a Kane County School District employee, I understand that the Laptop assigned to me remains the property of the Kane County School District (KCSD). *The* ***Laptop Use and Security Policy*** *outlined below will guide my use of this productivity tool.*

Article I: ***Security and Protection***

- I agree to read and follow the District's Acceptable Usage Policy.
- I understand that my Laptop needs to be with me at work every day and connected to the district network. (The network connection allows for regular anti-virus and Windows updates.)
- I understand that I am permitted to take my Laptop home at the end of the work day, or
- I will secure my Laptop in my classroom or office when not in use.
- I understand that leaving the Laptop in a car can promote theft and damage from temperature extremes, and that I will be responsible to pay for loss or damage as a result of leaving the laptop in a car.
- I understand that I am expected to protect my Laptop from damage and theft, and that I will be responsible for damage or theft that takes place off school district property.
- I agree to carry this laptop in a padded case or backpack, to minimize the chances that it will be damaged or destroyed.
- I understand that if my laptop is lost or stolen, I will immediately notify the District and file a report with the police.

Article II: Connectivity at Home

- I understand that this Laptop can be configured for use at home as well as at work. In order to configure at home connectivity,
- I understand that I must discuss my home ISP (Internet Service Provider) environment with authorized KCSD Information Technology (IT) personnel and provide specific information as needed.
- I understand that if I fail to provide information necessary for at-home connectivity, I will not be allowed to access my KCSD accounts from home.
- I understand that I am not to install ISP software on this computer. Installation of AOL is strictly prohibited.
- If I need ISP software installed, I will contact IT personnel for installation or permission to install.

Article III: User Interface at Home or School

- I understand that I may need to attend an orientation session to learn how to use my Laptop.
- I understand that I may use my school discretionary funds, where available, to purchase any necessary KCSD approved add-ons and storage devices (e.g. additional battery pack, mouse, monitor, pen drive) and that such purchases then become the property of the Kane County School District.
- I understand that I will not install any programs or applications onto my Laptop not approved by KCSD technology department.

- I understand that specialized academic software required by me or my students must be cleared by authorized IT personnel prior to purchase and installation.
- I understand that I will not permit students to use my Laptop, with the exception of classroom instruction or demo.
- I understand that this laptop computer will be in my possession at all times, i.e., I am not to lend my Laptop to anyone, including members of my family, for any reason.
- I understand that I am responsible for the appropriate use of my Laptop, including anything stored on the machine.
- I understand that I must return my Laptop to the school office if I resign or if I am planning an absence of more than two weeks. (not including summer break)
- I understand that all district Network Use Policies govern the operation of my laptop on and off the KCSD network.
- I understand that any repair will be handled through the KCSD IT team.
- I understand that I will not be held responsible for computer problems resulting from regular school-related use, but may be held responsible for any problems caused by my negligence as deemed by the District's administration.

APPROVED September 3, 2009 KANE COUNTY SCHOOL BOARD
POLICY EFF Revised