ACCEPTABLE USE POLICY

This policy incorporates the lawful protections required by the Child Online Protection Act (COPA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet Protection Act (CIPA), and the Neighborhood Children's Internet Protection Act (NCIPA), as may be applicable to the School and its contractors, and shall encompass local, Intranet and Internet networks and resources utilized by Board members, staff, students, parents/guardians and other users.

The Board of Directors supports use of local, intranet and Internet computer/resource networks in the School's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the School as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The electronic information available to students and staff does not imply endorsement of the content by the School nor does the School guarantee the accuracy of information received on the Internet. The School shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The following policy shall be followed with regard to the School's local, intranet and Internet computer/resource networks.

Definitions

Acceptable Use - utilizing School resources (network, computing devices or applications) to satisfy educational or administrative assignments, research or tasks described wholly as official Tillotson business in the context described in this policy.

Access to Internet - a computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet.

Authorized Account Owner - an individual authorized by the School to have access to and utilize computers/networks and/or services owned, leased or operated by the School.

Blog - short for Web Log; a web page that serves as a publicly accessible personal journal for an individual (Blogger). Typically updated daily, blogs often reflect the personality of the author.

Child Pornography - the term child pornography shall have the meaning given such term in section 2256 of Title 18, United States Code.

Computers - any and all computers, computer equipment, systems, hardware and/or software owned, leased or operated by the ACLD Tillotson School.

Direct Electronic Communications - any and all communications made or disseminated by electronic means, including but not limited to electronic mail, chat rooms or other forms of direct electronic communications.

Fair Use Guidelines - guidelines developed by the School to clarify the application of fair use principles for educators considering digital copyright issues.

Hacking - the act of accessing or attempting to access targeted network resources, either internal or external, for the purpose of gathering/acquiring nonprivileged access and/or information, passwords, functionality, identity theft or distribution of unsolicited scripts and/or viruses.

Harmful to Minors - any picture, image, graphic image file, or other visual depiction that taken as a whole and with respect to minors appeals to the prurient interest, depicts, describes or represents in a patently offensive way an actual or simulated sexual act or sexual conduct, as described by the Children's Internet Protection Act, and taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

Inappropriate Matter - in addition to items defined under "Harmful to Minors," any material that contributes to intimidation, constitutes a safety/security concern, threatens, is deemed as tasteless by the School's filtering application or violates any existing School policy, including but not limited to policies relating to Human Relations, Sexual Harassment and/or Student Code of Conduct.

Inappropriate Usage of School Computers/Internet/Hardware and Software Resources - use of the School's computers and local, intranet and Internet services, owned, leased or operated, that violates the School's policy on Internet usage and safety or conflicts with the School's mission and purpose or with an employee's authorized job duties or responsibilities. The school or office administrator shall have the authority to determine what is considered to be inappropriate use. Issues related to inappropriate use will be overseen by a steering committee.

Individuals Covered by This Policy - Board members, staff, students, parents/ guardians and other users of computers/resource networks and/or services owned, leased or operated by the ACLD Tillotson School.

Instant Messaging - abbreviated IM, a type of service that enables users to communicate in real time over the Internet. Typically, the IM system alerts users whenever someone from their private list is online and a chat session can be initiated with that individual.

Internet - defined as the "standard" Internet (the collaboration and interconnectivity of computer networks and resources worldwide) and Internet2 (a higher educational/research form of noncommercial Internet access).

Local, Intranet and Internet Computer Networks -

1. Networks residing within the boundaries of a School-owned/leased facility.
2. Leased/Owned interconnecting networks under the School's management.
3. Outside, non-School-owned/operated networks and corresponding resources.

Minor - an individual who has not attained the age of eighteen (18).

Obscene - the term obscene has the meaning given such term in section 1460 of Title 18, United States Code.

Online - active connection to network hardware, software or service resources.

Rogue Access - interpreted by the School as any connectivity to any School resources via internal network access (through devices, hard-wired drops or wireless) or external network access (Internet, Internet2, wireless, dial-in, VPN, or satellite) without explicit permission obtained from the Executive Director or designee.

Rogue Devices or Applications - hardware devices or software not authorized by the Executive Director or designee to be utilized on School network infrastructure or computers.

Sexual Act; Sexual Contact - the terms sexual act and sexual contact have the meanings given such terms in section 2246 of Title 18, United States Code.

Spam - a slang term for e-mail that is the electronic equivalent of junk mail; usually advertisements, jokes or notices of no real value to the recipient.

Technology Protection Measure - specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of Title 18, United States Code.
2. Child pornography, as that term is defined in section 2256 of Title 18, United States Code.
3. Harmful to minors.

Vandalism - any malicious attempt to harm or destroy the School's computers, data, applications, and/or network functionality or the data and/or functionality of another user's computer. This includes but is not limited to the uploading or creation of computer viruses.

World Wide Web - a collection of Internet sites that offer text and graphics and sound and animation resources through the hypertext transfer protocol. It is often abbreviated "WWW" or called "the Web."

Safety Procedures

All Internet access on School-owned/leased resources will be filtered through the use of filtering software to prevent access by minors/parents/guardians/staff/outside users to inappropriate matter on the Internet and World Wide Web.

In order to restrict the access of minors/parents/guardians/staff/outside users to visual depictions that are obscene, child pornography, and other materials harmful to minors, filtering software will be utilized on all School computers with access to the Internet.

An administrator, supervisor, or other person authorized by the School may request disabling a particular site from the filtering software, during use by an adult, in order to enable access for bona fide research or other lawful purpose.

Students will not be advised or encouraged by school staff to obtain free e-mail accounts through commercial providers (e.g., Hotmail, etc.) for use in class projects.

The School does not endorse or advocate the use of commercial Instant Messaging service and is not responsible for its content. Users shall not communicate electronically or agree to meet in person with unknown online acquaintances.

All individuals covered by this policy shall not participate in hacking or other unlawful online activities.

All individuals covered by this policy shall not while online disclose, use or disseminate personal identification information regarding minors or other users.

In a further attempt to ensure the safety and security of users, the online activities of users can/will be monitored and recorded.

The Executive Director or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.

Usage Procedures

Network accounts shall be used only by the authorized owner of the account for its authorized purpose. Certain communications and information accessible via the network may be confidential and disclosures of such information shall only be made where legally permissible. Network users shall respect the privacy of other users on the system.

The School will also implement network information security procedures that are incorporated into these guidelines by reference.

Students, staff and other School resource users are expected to act in a responsible, ethical and legal manner in accordance with School policy, accepted rules of network, usage and federal, state and local law.

The following types of usage are specifically prohibited and if performed will subject the user to certain consequences, including but not limited to loss of access and/or other disciplinary and/or legal actions:

1. Use of the network to facilitate any illegal activity including “hacking.”

2. Use of the network and/or its resources for commercial or for-profit purposes.

3. Use of the network and/or its resources for nonwork or nonschool-related work.

4. Use of the network and/or its resources for product advertisement or political lobbying.

5. Use of the network and/or its resources for harassment, hate mail, discriminatory remarks, bullying and offensive or inflammatory communication.

6. Unauthorized or illegal installation, downloading, distribution, reproduction, or use of copyrighted materials, i.e., plagiarism.

7. Use of the network and/or its resources to access obscene, pornographic material, or other material harmful to minors.

8. Use of inappropriate language or profanity on the network and/or its resources.

9. Use of the network and/or its resources to transmit material likely to be offensive or objectionable to recipients, including but not limited to spam.

10. Use of the network and/or its resources to intentionally obtain or modify files, passwords, and data belonging to other users, internal or external to the School's network.

11. Impersonation of another user, anonymity, and pseudonyms, i.e., identity theft.

12. Use of network facilities for fraudulent copying, communication or modification of materials in violation of copyright laws.

13. Copying, loading or use of unauthorized or pirated games, programs, files, data or other electronic media.

14. Use of the network and/or School resources to disrupt the work of other users.

15. Destruction, modification, vandalism or abuse of network hardware, software and/or functionality.

16. Quoting personal communications in a public forum without the original author's prior consent.

17. The creation of links to other networks whose content or purpose would tend to violate this policy or its guidelines.

18. Attaching rogue devices or applications to School resources.

19. Sending unsolicited e-mail for the purpose of advertisement or non-School business.

20. Installation and/or use of non-School authorized remote desktop or other computing utilities.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or School files. To protect the integrity of the system, the following security guidelines shall be followed:

1. Only current staff, students, parents/guardians and approved outside users are authorized to have accounts on the network.

2. Employees, students, parents/guardians and approved outside users shall not reveal their passwords to another individual.

3. Users are not to use a computer that is actively logged in under another user's name.

4. Any user identified as a security risk or having a history of problems with other computer systems, resources and/or networks may be denied access to the network.

5. No student shall ever be permitted to use/operate ANY staff computer for ANY reason.

6. All users must comply with the School's password requirements.

7. All users must utilize the School's guidelines for Virus Protection, Information Security, E-mail Accounts, Internet and Web Site Development Safety.

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator. Correspondingly, the appropriate administrator should report the activity to the Executive Director or designee.

Network users shall not reveal personal addresses, telephone numbers or any personal identification information about themselves or other users.

Copyright

The illegal use of copyrighted software by users is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

Responsibilities

The School shall make every effort to ensure that this educational resource is used responsibly by students, parents/guardians, staff and approved outside users.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

All users have the responsibility to respect and protect the rights of every other user in the School and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use. Issues related to inappropriate use shall be referred to the Executive Director or designee for review.

Illegal Activities

Users shall not attempt to gain unauthorized access (hacking) to the School's network resources (equipment or applications) either internally through the School's network or an outside non-School network. This prohibition includes intentionally seeking information about passwords ("password

cracking") belonging to other users, modifying passwords belonging to other users or attempting to log in through another person's account. Further, users may not attempt to access, copy or modify another user's files. These actions are not permitted and are illegal, even if only for the purposes of "browsing."

Users shall not go beyond their authorized access and permission level granted by the School.

Users shall not attempt to subvert network security, impair the functionality of the network or bypass restrictions set by the Executive Director or designee.

Users are also prohibited from destroying or vandalizing data, software or equipment.

Users shall not introduce or propagate computer viruses or worms.

Users shall not use any School resource to engage in any other illegal act.

Consequences for Inappropriate Use

The network user shall be responsible for vandalism and/or other damages, including lost/extended resource time of technology staff or outside contractors, affecting the equipment, systems, software and functionality resulting from deliberate or willful acts.

Illegal use of the network, intentional deletion/manipulation or damage to files or data belonging to others, copyright violations or theft of services and/or identity will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using School computers, network hardware/software resources and/or the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary and/or legal actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes but is not limited to the uploading or creation of computer viruses.

Further Provisions

It should be noted that all School computers, leased or owned, are the property of the School and are to be utilized as a tool to assist in education and job duties. No right of personal usage extends to the end-user in regards to private property.

The Board confirms through this policy that use of the Internet is a privilege, not a right; and that inappropriate, unauthorized and/or illegal use will result in the cancellation of those privileges and appropriate disciplinary/legal action.

The School reserves the right to log network use, to monitor fileserver space utilization by School users, to restrict access to external network sites and to monitor e-mail usage, while respecting the limited privacy rights of School users.

The School shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The School shall not be responsible for restoring any personally installed applications or data deemed as having no educational value.

The School reserves the right to re-image any School-owned/leased computer at its discretion.

The School shall not be responsible for any unauthorized charges or fees resulting from a user's ability or inability to access the Internet.

This policy in no way affects the duties and/or responsibilities of the School under the Family Educational Rights and Privacy Act (FERPA) and any other guidelines or policies relating to the management of student records.