USE OF TECHNOLOGY AT UNIVERSITY ACADEMY

This policy was adopted by the Board of Directors of the University Academy Charter School on November 27, 2006. It is effective from this date.

University Academy ("UA" or "the school" in this document) recognizes the educational and professional value of information technology as a means to access useful information and develop essential student skills; the school's technology exists to serve these purposes. University Academy expects all students and employees to use its technology resources responsibly. Disruptive, inappropriate, or illegal use of the school's technology resources shall not be tolerated.

Definitions

For the purposes of this policy, the following terms are defined:

User -- any person including (but not limited to) students, employees, Board members, and agents of the school, who is permitted by the school to utilize any portion of the school's technology resources.

Username -- any identifier that would allow a user access to the school's technology resources, including (but not limited to) e-mail and Internet access.

Password -- a unique sequence of characters used to authenticate a username as belonging to a user.

Administration of School Technology

The superintendent or his/her designee shall create and promulgate rules and procedures governing technology usage as necessary to support

the school's technology policies. The superintendent or his/her designee shall also assign trained personnel to maintain the school's technology so as to protect the school from liability and will protect confidential student and employee information retained or accessible through technology resources. Administrators of computer resources may suspend access to and/or availability of the school's technology resources to diagnose and investigate network problems or potential violations of the law or school policies, regulations and procedures.

Network Security

Use of the school's technology resources is a privilege, not a right. Users must adhere to school policies, regulations and procedures. No student, employee or other potential user will be given a username, password or other access to school technology if he/she is considered a security risk by the superintendent or his/her designee.

User Agreement and Privacy

All users must have an appropriately signed User Agreement on file with the school before they are allowed access to school technology resources, unless otherwise authorized by the superintendent or his/her designee. All users must agree to follow the school's policies, regulations and procedures. In addition, users must acknowledge that they do not have a legal expectation of privacy in their electronic communications or other activities involving the school's technology resources.

Content Filtering and Monitoring

The school will monitor the online activities of minors and operate a technology protection measure ("filtering/blocking device") on the network and/or all computers with Internet access, as required by law. The filtering/blocking device will be used to protect against access to visual depictions that are obscene, harmful to minors and child pornography, as required by law. Because the school's technology is a shared resource, the filtering/blocking device will apply to all computers with Internet access in the school.

Filtering/Blocking devices are not foolproof, and the school cannot guarantee that users will never be able to access offensive materials using school equipment. Evasion or disabling, or attempting to evade or disable, a filtering/blocking device installed by the school is prohibited.

The superintendent, designee or the school's technology administrator

may disable or reconfigure the school's filtering/blocking device to enable an adult user access for bona fide research or for other lawful purposes. In making decisions to disable or alter the school's filtering/blocking device, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the school.

Closed Forum

The school's technology resources are not a public forum and are to be considered a closed forum to the extent allowed by law. The school's web page will provide information about the school, but will not be used as an open forum. All expressive activities involving school technology resources that might reasonably be perceived to bear the imprimatur of the school and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school for legitimate pedagogical reasons. All other expressive activities involving the school's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

SAFE TECHNOLOGY USE

Student Users

No student will be given access to the school's technology resources until the school receives a User Agreement signed by the student and the student's parent(s), guardian(s) or person(s) standing in the place of a parent. Students who are at least 18 years old or otherwise able to enter into an enforceable contract may sign the User Agreement without additional signatures. The superintendent or designee has discretion to grant students, without a parent-signed User Agreement on file, permission to use school technology.

Employee Users

No employee will be given access to the school's technology resources until the school receives a User Agreement signed by the employee. Authorized employees may use the school's technology resources for reasonable, incidental personal purposes as long as the use does not violate any

provision of school policies, regulations or procedures, hinder the use of the school's technology for the benefit of its students, or waste school resources. Any use that jeopardizes the safety, security or usefulness of the school's technology or interferes with the effective and professional performance of the employee's job is considered unreasonable. Because computers are shared resources, it is not appropriate for an employee to access, view, display, store, print or disseminate information via school resources, including e-mail or Internet access, that is not appropriate for students or other authorized users.

Board Member Users

Members of the Board may be granted user privileges, including an e-mail address, upon completion of a User Agreement. Board members are subject to school policies, regulations and procedures on technology use and must also comply with the Missouri Sunshine Law.

External Users

Consultants, counsel, independent contractors, and other persons having a professional or volunteer relationship with the school may also be granted user privileges at the discretion of the superintendent or his/her designee, subject to completion of a User Agreement; and for the sole, limited purpose of conducting activities pertinent to the mission of the school. External users must abide by all laws, school policies, regulations and procedures.

Privacy

All school technology resources are considered school property. The school may remove, change or exchange hardware or other technology, load or delete new programs or information, install new equipment, enter any system to correct problems, or upgrade any system at any time without prior notice. The school may examine all information stored on school technology resources at any time and may monitor employee and student technology usage. School administrators or their designees may access or search electronic communications, all data stored on the school's technology resources, and downloaded material, including files deleted from a user's account, at any time.

Violations of Technology Usage Policies and Procedures

A user's privileges may be suspended pending an investigation con-

cerning use of the school's technology resources. Any violation of school policies, regulations or procedures regarding technology use may result in temporary, long-term or permanent suspension of user privileges. The administration may use disciplinary measures to enforce school policies, regulations and procedures. Employees may be disciplined or terminated, and students suspended or expelled, for violating the school's policies, regulations and procedures. Any attempted violation of school policies, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Damages

All damages incurred by the school due to misuse of the school's technology resources, including the loss of property and staff time, will be charged to the user. School administrators have the authority to sign any criminal complaint regarding damage to school technology.

General Rules and Responsibilities

The following rules and responsibilities apply to all users of school technology resources:

1. Applying for a username under false pretenses is prohibited, using another person's username and/or password, and sharing one's username and/or password with any other person are all prohibited. A user will be responsible for actions taken by any person using the username or password assigned to the user.
2. Deleting, examining, copying or modifing files and/or data belonging to other users without their prior consent is prohibited.
3. Mass consumption of technology resources that inhibits use by others is prohibited.
4. Noneducational Internet usage is prohibited, unless authorized by the school.
5. Use of school technology for soliciting, advertising, fundraising, commercial purposes or for financial gain is prohibited, unless authorized by the school.
6. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
7. Users are required to obey all laws, including criminal, copyright pri-

vacy, defamation and obscenity laws. The school will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using school technology in violation of any law.

8. Accessing, viewing or disseminating information using school resources, including e mail or Internet access, that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, is prohibited.
9. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of school staff for curriculum-related purposes.
10. Accessing, viewing or disseminating information using school resources, including e mail or Internet access, that (1) constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g., defamation of character or threats of violence); (2) is likely, because of its content or manner of distribution, to cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or (3) will cause the commission of unlawful acts or violate school regulations is prohibited.
11. Any use that has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy, or sexual orientation, or that violates any person's rights under applicable laws, is prohibited.
12. Any unauthorized, deliberate or negligent action that damages or disrupts technology is prohibited, regardless of the location or the duration of the disruption.
13. Users may only install and use properly licensed software, audio or video media purchased by the school or approved for use by the superintendent or his/her designee. Copying for home use is prohibited unless permitted by the school's license and approved by the school. School technology software may not be removed from the school premises unless authorized by the school.
14. All users must use the school's property as it was intended. Technology hardware may not be lifted, moved or relocated without permission from an administrator.

Technology Security and Unauthorized Access

The following acts are prohibited:

1. Use of school technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another;
2. The unauthorized copying of system files;
3. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any school technology;
4. Any attempts to secure a higher level of privilege on the technology resources without authorization;
5. The introduction of computer "viruses," "hacking" tools or other disruptive/destructive programs into a school computer, network or any external networks.

All users shall immediately report any security problems or misuse of the school's technology resources to a teacher or administrator.

Online Safety - Disclosure, Use and Dissemination of Personal Information

Users shall receive or transmit communications using only school-approved and school-managed communication systems. For example, users may not use web-based e-mail messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the school.

Students

The school will instruct students on the dangers of sharing personal information over the Internet. Unless authorized by the school, student users are prohibited from sharing personal information about themselves or others over the Internet. A student user shall promptly disclose to his or her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable. Students shall not agree to meet with someone they have met online without parental approval. No curricular or noncurricular publication distributed using school technology will include the address, phone number or e-mail address of any student without permission.

Employees

All school employees shall abide by state and federal law, Board policies and school rules when communicating information about personally identifiable students. Employees shall not transmit confidential student information using school technology unless designated for that use. Em-

ployees must also take precautions to prevent negligent disclosure of student information or student records.

Electronic Mail

Users must adhere to the same standards for communicating online that are expected in the classroom and that are consistent with school policies, regulations and procedures. Forgery or attempted forgery of e-mail messages is illegal and is prohibited. Unauthorized attempts to read, delete, copy or modify e-mail of other users are also prohibited.

Exceptions

Exceptions to school rules will be made for school employees or agents investigating a use that potentially violates the law or school policies, regulations or procedures. Exceptions will also be made for technology administrators who need access to school technology resources to examine, maintain or modify them.

Waiver

Any user who believes he or she has a legitimate reason for using the school's technology in a manner that may violate any of the school's policies, regulations or procedures may request a waiver from the superintendent or designee. In making the decision to grant a waiver to a student, the administrator shall consider the purpose, age, maturity and level of supervision involved.

No Warranty

The school makes no warranties of any kind for the technology services, products or access it provides. The school is not responsible for loss of data, delays, nondeliveries, misdeliveries or service interruptions. Nor does the school guarantee the accuracy or quality of information obtained from the Internet or use of its technology resources.