SECTION: C – General School Administration
POLICY TITLE: Computer and Electronic Device Use
FILE NO.: CC
DATED: May 18, 2021

TABLE OF CONTENTS

1. PURPOSE AND PHILOSOPHY

The Utah County Academy of Sciences' (UCAS) Board of Trustees believes that computer use is a valuable and necessary component of a UCAS student and employee's work. In addition, varying work responsibilities result in access to information from sources such as software programs, the Internet, the UCAS network, etc. Access and authorization to the UCAS computer systems and information carry a corresponding responsibility to their appropriate use.

Annually, every student and employee will be required to sign this Acceptable Use Agreement found in CC – Form A.

2. DEFINITIONS

2.1. Electronic devices include, but are not limited to:

2.1.1. Beepers,

2.1.2. Pagers,

2.1.3. Cell phones, with and without picture taking capacity,

2.1.4. Blackberries,

2.1.5. I-Phones; and

2.1.6. Hands-free devices (Bluetooth)

3. ACCESS

3.1. The Utah County Academy of Sciences (UCAS) may provide computers, networks, and filtered Internet access to support the educational mission of the school and to enhance the curriculum and learning opportunities for students and employees. The internet service at UCAS is

provided and monitored by the Utah Education Network (UEN) as a public service.

3.2. Access and use of the school's computers, networks, and Internet access is provided for administrative, educational, communication, and research purposes consistent with the school's educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to the use of the school's computers, networks, and Internet access.

3.3. UCAS students and employees are to utilize the school's computers, networks, and Internet access for educational purposes, the performance of job duties, and professional or career development activities. Incidental personal use by students and employees of the school's computers, networks, and Internet access is permitted as long as such use does not:

3.3.1. interfere with the student's education or the employee's job duties and performance;

3.3.2. interfere with computer system operations; and/or

3.3.3. interfere with other computer system users.

3.4. "Incidental personal use" is defined as use by an individual student or employee for occasional personal communication and information.

4. SYSTEM SECURITY

The school utilizes an Internet filtering system to assist in restricting access to Internet sites containing material that is obscene, pornographic, or harmful to minors. Even though the school and the UEN take reasonable efforts to block material that is obscene, pornographic, or harmful to minors, no filtering system or features will filter out all obscene, pornographic, harmful, or inappropriate material. It is the responsibility of the computer system users to maintain a high level of integrity to protect themselves and others from such inappropriate material. As used herein, references to the terms "obscene," "obscenity," "pornographic," "pornography," "child pornography", and "harmful to minors" are defined by applicable state and federal laws, regulations, and cases.

5. PROHIBITED ACTIVITIES

5.1. Each student, employee, or other computer system user is responsible for his/her actions and activities involving the school's computers, networks, and Internet access, and for his/her computer files, passwords, and accounts. General examples of unacceptable uses which are expressly prohibited include, but are not limited to, the following:

5.1.1. Any use that is illegal or in violation of Board of Trustees policies and/or administrative procedures, directives, or rules, including, but not limited to, bullying, harassment, discrimination (i.e., race, color, gender, nationality, religion, age, or disability), defamation, violent or threatening communications and behavior, infringement of copyright or trademark laws, offering for sale, purchase, or use of any prohibited or illegal substances, etc.

5.1.2. Any use involving obscene, pornographic, sexually explicit, sexually suggestive, or any other harmful or inappropriate material.

5.1.3. Any inappropriate communication that is obscene, profane, lewd, vulgar, belligerent, inflammatory, or threatening.

5.1.4. Any use for private or commercial financial gain, advertising, or solicitation purposes.

5.1.5. Any use as a forum to solicit, proselytize, advocate, or communicate the views of an individual or a non-school sponsored organization, to solicit membership in or support

of any non-school sponsored organization, or to raise funds for any non-school sponsored purpose, whether for profit or not for profit.

5.1.6. Any communication that represents personal views as those of the school or that could be misinterpreted as such.

5.1.7. Downloading or loading copyrighted or illegal software or other hazardous applications or files is prohibited. Downloading network wide software is allowed only with written permission from the school principal or other appropriate administrator.

5.1.8. Any student use of Internet chat rooms except when monitored as a class activity.

5.1.9. Any unauthorized attempt to bypass the school Internet filtering systems and features.

5.1.10. Any malicious use or disruption of the school's computers, networks, and Internet access or breach of security features.

5.1.11. Any physical or electronic vandalism to the computer system or equipment.

5.1.12. Failing to report a known breach of computer security or violations of this Policy to the school principal or other appropriate administrator.

5.1.13. Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates Board of Trustees policies and/or administrative procedures, directives, and rules.

5.1.14. Using the school's computer network or Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access.

5.1.15. Any use involving damaging, dangerous, or disruptive material.

5.1.16. Any use involving personal or generalized attacks or harassment, or to communicate false or defamatory information.

5.2. The foregoing list provides general guidelines and examples of prohibited uses for illustrative purposes, but does not attempt to state all required or prohibited activities by computer system users. Students, employees, and other computer system users who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the school's principal or other appropriate administrator.

5.3. The school retains control, custody, and supervision over all computers, networks, and Internet access owned, licensed, or leased by the school. The school reserves the right to monitor all computer and Internet activity by students, employees, and other computer system users. Students, employees, and other computer system users have no expectation of privacy in their use of the school's computer system and equipment.

5.4. Employees and other computer system users are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. Employees and other computer system users with access to student records may not use, release, or share these records, except as authorized by federal and state law.

5.5. For personal safety purposes in using the school's Internet access, computer system users are advised not to disclose personal information such as home addresses, home telephone numbers, social security numbers, etc.

5.6. The Utah State Core Curriculum requires students to become effective and efficient users of online resources. Students need access to e-mail and the Internet to meet these requirements. Employees and volunteers assigned to supervise student use of computers must insure compliance with this Policy. Although student use of the school's computer system at school will be generally supervised by school staff, UCAS cannot guarantee that students will not gain access to inappropriate material. The school encourages parents/legal guardians to have a discussion with their students about values and how those beliefs should guide student activities while using the school's computers, networks, and Internet access.

5.7. All computer system users shall be responsible for any and all claims, losses, damages, or costs (including attorneys' fees) associated with their use of the school's computers, networks, and Internet access, including, but not limited to, illegal uses, copyright and trademark violations, defamation, discrimination, harassment, etc. All computer users shall hold harmless and indemnify the school and its employees and agents from such claims, losses, damages, and costs.

5.8. The school assumes no responsibility for any unauthorized charges made by computer system users, including, but not limited to, credit card charges, subscriptions, long distance telephone charges, equipment and line costs, etc., and shall hold harmless and indemnify the school and its employees and agents from such unauthorized charges.

5.9. The school makes no warranties of any kind, either expressed or implied, that the functions or the services of the computer system provided by or through the school will be error-free or without defect. The school will not be responsible for any damage users may suffer, including, but not limited to, loss of data or interruptions of service. The school is not responsible for the accuracy or quality of the information obtained through or stored on the computer system.

5.10. Access and use of the school's computers, networks, and Internet access is a privilege and not a right. This privilege may be revoked at any time for failure to comply with the terms and conditions of this Policy and/or applicable administrative procedures, directives, and rules.

5.11. Any student who violates this Policy and/or applicable administrative procedures, directives, and rules governing the use of school computers will be subject to disciplinary action, such as losing computer use privileges, suspension, and expulsion. The introduction of a computer virus to the school network, whether intentional or unintentional may result in the student, his/her parents, or a staff member being charged for the repair of the system. Illegal uses by students of school computers will also result in referral to law enforcement authorities.

5.12. Any employee who violates this Policy and/or applicable administrative procedures, directives, and rules governing the use of school computers will be subject to disciplinary action, up to and including employment termination. Professionally licensed employees may be referred to the Utah Professional Practices Advisory Commission (UPPAC), along with any and all evidence, for investigation and possible disciplinary action against professional licensing. Illegal uses by employees of school computers will also result in referral to law enforcement authorities.

5.13. Annually, each employee authorized to access the school's computers, networks and Internet access is required to sign an "Employee Computer Use Agreement" stating that they have read the Agreement, this Policy, and Administrative Procedures, and agree to comply with the terms and conditions set forth therein. The "Employee Computer Use Agreement" will be retained in the employee's school file.

5.14. Each school year, every student authorized to access the school's computers, networks, and Internet access shall be required to provide the school a "Student Computer Use Agreement" signed by the student and a parent/legal guardian stating that they have read the Agreement, this Policy, and Administrative Procedures, and agree to comply with the terms and conditions set forth therein.

5.15. Notice of the availability of this Policy shall be posted in a conspicuous place within the school.

6. PERSONAL ELECTRONIC DEVICES

6.1. Electronic devices, whether personal or school issued, may be used during the school day or during school-sponsored activities as follows:

6.1.1. Students may have electronic devices in their possession during the regular school day.

6.1.2. The devices must remain out of sight during instructional time and be turned off or on a silent mode.

6.1.3. If students intentionally use or respond to electronic devices during instructional time or during time identified by teachers, electronic devices may be confiscated.

6.1.4. Devices may be retrieved by individuals designated by the school. Students may also be subject to school discipline.

6.1.5. UCAS Administration shall establish a warning schedule for student violations which all school employees shall follow (see student handbook). Exceptions may be made for individual students or for specific time periods as warranted. Time periods shall be interpreted with flexibility.

6.1.6. Electronic devices must be either turned off of held in a secure place by the teacher, as determined by individual teacher, during class quizzes, tests and standardized assessments.

6.1.7. Electronic devices inappropriately used or disclosed may be subject to search by school administration based on reasonable suspicion.

6.2. Exceptions to general electronic device policy shall be made consistent with UCAS policies, but in the judgment and discretion of individual teachers. Some exceptions include, but are not limited to:

6.2.1. Medical reasons - School administrators may give permission for students to possess electronic devices for good cause shown if the devices do not distract from the instructional or education process.

6.2.2. Parent request - Parent(s) may request that a student possess an electronic device on active mode at all times during the school day , with the exception of during course or subject tests and standardized assessments. Teachers shall grant such requests for good cause shown. (Good cause may include medical needs or unusual family situations.)

6.2.3. Teacher permission - A teacher may permit a student to have an electronic device in his possession at all times during a regular school day, including during assessments, based on a written §504 plan, an IEP or legitimate circumstances as determined by the individual teacher.

6.2.4. Emergency - Students may use electronic devices in situations that threaten the health, safety or well–being of students (including themselves), school employees or others.

6.2.5. Parents shall make requests for exceptions to this policy in writing to the school principal, designee or individual teacher.

7. CONSEQUENCES FOR VIOLATION OF THIS POLICY

7.1. A will receive one warning prior to discipline for violation of this policy, as determined by the school.

7.2. Designated individuals, upon identification, may retrieve their child's electronic device during school hours or by appointment.

7.3. A school may impose other consequences for a student's violation of the electronic device policy only following notice of such policy to the school community. Such penalties are not exhaustive and more than one penalty may be imposed, if warranted. Such penalties may include:

7.3.1. loss of electronic device privileges

7.3.2. disciplinary letter

7.3.3. in-school suspension

7.3.4. suspension

7.3.5. loss of extracurricular or honor privileges or recognition

7.3.6. If students are defiant and will not cooperate with school administrators and/or will not surrender electronic device(s), the designated school administrator may take appropriate action for the safety and well-being of the student and other students or employees at the school. The school principal or designee shall notify a parent immediately of additional penalties.

8. CONFISCATED ELECTRONIC DEVICES

8.1. Only licensed UCAS personnel (unless other employees are specifically identified in policy) may confiscate student electronic devices.

8.2. Licensed UCAS employees are discouraged from searching or reviewing material or numbers stored on student electronic devices except under compelling circumstances.

8.3. Licensed UCAS employees may search an electronic device if the device is found by the employee for the limited purpose of determining the device's owner.

8.4. UCAS will do their best to guard and protect confiscated electronic devices, but are not responsible for loss, damage, theft.

8.5. UCAS will make a good faith effort to notify parent(s) or designated individuals that electronic device is in school's possession and, time and resources permitting, will maintain electronic devices until the end of the school year. Prior to disposal of devices, schools/school districts shall clear all personal data.

9. OTHER PROVISIONS

9.1. Picture taking or recording by students is strictly forbidden in school or school activity private areas, such as locker rooms, counseling sessions, washrooms, and dressing areas.

9.2. Students bring electronic devices on school property or to school activities at their own risk. The school is not responsible for lost, stolen or damaged electronic equipment.

9.3. Students are strictly responsible for their own electronic devices. If devices are borrowed or taken

and misused by non-owners, device owners are jointly responsible for the misuse or policy violation(s).

9.4. Students and parents should be informed and understand that confiscated electronic devices may be subject to search by school officials.

9.5. A student's penalties for violation(s) of an electronic device policy provision may vary depending upon the intentional nature of the violation, other disciplinary actions the student may have received and specific circumstances of the violation.

EXHIBITS
None

REFERENCES
UCAS POLICY JK
UTAH CODE ANN. § 53E-9-101, et seq.
UTAH ADMIN. CODE R277-495
CHILDREN'S INTERNET PROTECTION ACT OF 2000, AS AMENDED, 15 U.S.C. §6501, et seq. (P.L. 106-554).
Communications Act of 1934, as amended, 47 U.S.C. §254, et seq.
Elementary and Secondary Education Act of 1965, as amended, 20 U.S.C. §7001, et seq.

FORMS
Policy CC Form A – Employee Computer Use Agreement
Policy CC Form B – Student Computer Use Agreement

HISTORY
Revised – May 18, 2021. Section 2, 5 – 9 added.
Adopted– September 16, 2014.