



# Union County/ College Corner Joint School District

## Technology Acceptable Use Policy

### Student Agreement

Policy Approved by School Board August 13, 2012

Union County/College Corner Joint School District provides technology tools for the benefit of its staff and students. Students are responsible for good behavior on school computer networks just as they are in a classroom or school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. Simply, access to the network services and support of those services will be provided to students who agree to act in a considerate manner.

These technology tools are to be used primarily to support teaching and learning, in accordance with the policies and guidelines contained in this document. This Technology Acceptable Use Policy (AUP) addresses acceptable and unacceptable ways in which the student in our district may use the technology tools, and it addresses specific user responsibilities, rights and expectations.

However, given the rapidly changing nature of technology systems and services, the policies defined in this document cannot cover every possible situation. Therefore, in addition to the specific acceptable and unacceptable uses presented, this AUP provides general principles which shall direct the use of Union County/College Corner Joint School District technology tools. Put another way, students and adults are expected to use good judgment when working in gray areas not covered explicitly by the rules.

Adherence to this policy shall be the joint responsibility of the students, parents and employees of Union County/College Corner Joint School District. A signed AUP is required before a school network user account can be set up.

### **Bring your Own Technology Guidelines**

The Union County/College Corner Joint School District offers the “Bring Your own Technology” (BYOT) program to current **Sophomore, Junior and Senior students**. This program allows **Sophomore, Junior and Senior** students the ability to attach personal electronic devices to the school’s wireless network. It is our hope that students will be able to use this freedom of choice to identify and use the tools that allow them to pursue their own personalized educational and technological experience within the school district’s environment. With the convenience and capability of this privilege comes an increased responsibility on the part of the community members to use personal and school owned tools appropriately and with consideration of others in mind. The following devices will be allowed; Kindle Fire, iPads, netbooks, laptops, Microsoft Tablets, and Galaxy Tablets. Any device not listed, must be approved through the building principal or the Technology Department. Devices may or may not be used in each classroom at the teacher’s discretion.

Students using privately owned electronic devices must follow the policies stated in this document while on school property, attending any school-sponsored activity, accessing UC/CC JSD’s provided resources, using the UC/CC JSD’s network or while interacting in real or delayed time with UC/CC JSD community members. Use of these devices gives tacit approval for school IT personnel and faculty/administrators to observe and utilize the devices to confirm compliance with school policies described.

In the classroom environment, the teacher or other designated adult is the determiner of appropriate and inappropriate use of technology. Teachers may declare technology-free times, call for the

placing of technology at the front of the room or in a ready-to-use position. It is inappropriate to attempt to covertly use technology or overtly use technology in ways that are inappropriate, not indicated by the instructor or that run counter to the educational purpose of the class. No intra- or inter-class communication is authorized between students except as designated and/or supervised by an adult for a specific time period.

Electronic devices should be used in the building following guidelines that promote the utmost respect of decency, civilized behavior, and common courtesy. Devices should not be used to conduct audio/video conversations except in authorized areas or with the specific permission of an adult. Notifications and other alerts should be set to silent or vibrate at all times unless requested by an adult.

Use of personal or school communications tools, including but not limited to chat, telephone, e-mail, texting, social networking should follow guidelines of personal decency and decorum. Inappropriate language, harassing behavior, overtly sexual or violent behavior or innuendo is a violation of the letter and spirit of the rule and may be subject to disciplinary action.

Personal electronic devices should not be used in violation of any school policy or direction given by a classroom teacher or other UC/CC JSD employee. Use of personal electronic devices for entertainment or recreational use may be severely limited by UC/CC JSD staff, teachers or administrators based on the level of distraction and/or network resources used.

Any device used or operated in an unauthorized manner may be taken and held in the principal's office until a parent or guardian picks them up and may result in the user being subject to other disciplinary consequences.

### **Privileges and Acceptable Use**

We hope that students find UC/CC JSD's technology tools to be useful assets that assist them in achieving their educational goals. A school network user account grants a student access to:

- Productivity software (Word, PowerPoint, etc.) and various departmentally used pieces of software
- The Internet and many subscribed Internet reference and tutorial resources (which are accessible from any student computer in the building and in many cases on personal electronic devices at home)
- Note taking and bibliography applications

### **Users are encouraged to:**

- Use technology tools to support their learning in ways that are consistent with the mission of the school;
- Conduct research using the Internet for instructional purposes related to class curriculum and personal interest and development;
- Access information that will facilitate their selection of the college or university they want to attend;
- Increase their awareness of career path opportunities;
- Infuse technology into their course work;
- Improve their information literacy and research skills;
- Find ways to use technology for service to others.

## **Security**

Security on the UC/CC JSD network is a priority. Anyone identifying a security problem on the network should notify a teacher or the Technology Department. If you find a problem you should not demonstrate the problem to other users or try to bypass the problem by using another individual's user account. Users may not access accounts or password that belong to other users, or misrepresent other users on the network. Unauthorized attempts to login to the network as a system administrator will result in cancellation of user privileges. Your device must be registered with the Technology Department before it is allowed on the network. The Technology Department will also install the schools antivirus program to aid in protecting the school network from viruses that may already be on the device. The antivirus program is free to all staff and students.

## **Unacceptable use**

The list of inappropriate uses of technology tools and accounts currently includes, but is not limited to the following. (This list may be updated at any time.)

- Using the Internet or school network for any illegal activity, including gambling, computer hacking (and all variations thereof) and copyright law violations
- Use of Anonymous Proxies, Caching Servers, or any other means to avoid restrictions placed on the UC/CC JSD network and/or internet access
- Gaining intentional access to materials, maintaining access to materials or distributing material which are obscene, pornographic or whose dominant appeal is sexual arousal
- Gaining intentional access to material, maintaining access to materials or distributing materials which utilize or encourage excessive use of violence, blood, gore, or the diminishment of the value of life
- Associating a website with the school without proper authorization or presenting the school name, logo, or identity in a formal or informal publication, document, or program without prior approval
- Downloading, installing or accessing unauthorized software or other executable files (e.g. .exe, .bat, .pif, .reg) without the permission of the UC/CC JSD staff; this includes but is not limited to the use of unauthorized operating systems or other root level programs that could be installed on school computers or devices
- Deliberately introducing a virus to, or otherwise improperly tampering with any district owned system
- Intentionally installing or accepting spyware, malware, or other disruptive, intrusive, or destructive programs
- Attempting to gain access to or gaining access to network hardware (including wall jacks, wires, switches, routers, servers, access points, etc.). This includes placing unauthorized devices onto the school's wired network.
- Obtaining or sending information that could be used to make destructive devices such as guns, weapons, bombs, explosive or fireworks
- Posting messages on or through the network or internet, including those that are anonymous, that use abusive or profane language, or the system to harass, insult or verbally attack others or disrupt normal function
- Using limited resources provided by the school in a wasteful manner
- Causing or contributing to the unnecessary congestion or malicious interference of the network
- Gaining unauthorized access to resources or files
- Identifying oneself with another person's name or password, account, or credentials (including guests)

- Providing access to the school's network to unauthorized individuals or granting limited authorizations to unauthorized people
- Using technology tools for financial or commercial gain (unless approved by UC/CC JSD administration for a school activity directly supervised by a staff member)
- Stealing or vandalizing data or equipment
- Invading the privacy of other individuals
- Attempting to gain access to or gaining access to student records, grades or files outside of the adult supervised and approved shared drives or individual authorized user account
- Degrading or disrupting equipment or system performance
- Failing to obey school or classroom technology use rules
- Taking part in any activity related to technology use, which creates a clear and present danger or a substantial disruption to the orderly operation of the school
- Use of school or personal electronic devices to perform unethical actions including, but not limited to, cheating, unauthorized collaboration, or plagiarism (e.g. cell phone texting answers or taking pictures of exams).

## **Risks**

The educational community of UC/CC JSD makes no warranties of any kind, whether expressed or implied for the service it is providing and is not responsible for any damages the user may suffer. This includes loss of data, non-deliveries, mis-deliveries, or service interruptions. The student is responsible for evaluation of any information obtained from the Internet. UC/CC JSD specifically denies any responsibility for the accuracy or quality of information obtained through its services. Additionally, UC/CC JSD will not be responsible for unauthorized financial obligations resulting from provided access to the Internet. The users of UC/CC JSD technology tools agree that they waive any right to privacy that they may have for such use (including personal devices). We may monitor the users of technology and many also examine all system activities in which the user participates. Users have no right to privacy as to any information or file created, maintained, transmitted or stored in or on UC/CC JSD's property, through our technical resources or on personal devices at school. Users should know that content which includes but is not limited to: sexual comments or images, racial slurs or other offensive comments, defamatory, discriminating or harassing materials distributed, accessed or downloaded through technology tools could expose them to legal liability as well as to disciplinary action.

## **Violations**

UC/CC JSD endeavors to create an atmosphere which fosters academic achievement, personal responsibility and respectful relationships among students, faculty, staff, administrators, families and other members of the UC/CC JSD community. Any behavior or action contrary to UC/CC JSD's purpose is considered an infraction and may result in the immediate and/or permanent loss of access to technology tools and/or further disciplinary actions. At any time, as required for administrative or technical reasons, a network administrator may close an account or revoke the privilege or bringing that device to school again. This infraction could also warrant revoking the privilege of using a school owned device as well.

