MCKINNEY ISD
TECHNOLOGY RESOURCES
STUDENT ACCEPTABLE USE POLICY

Technology resources, including Internet access, will be used to promote innovation and educational excellence consistent with the Texas Essential Knowledge and Skills and the goals of McKinney Independent School District ("McKinney ISD" or "District"). The District has deployed a wide-area network as well as access to the Internet to provide students with access to a multitude of instructional resources. This also places ethical responsibilities on all technology users, including students.

Students are responsible for appropriate behavior on District computer networks just as they are in a District classroom or hallway. Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of McKinney ISD activities. Communications on the network are often public in nature. General school rules and standards of student conduct as stated in the existing Student Code of Conduct, Board Policies, and this Technology Resources Student Acceptable Use Policy ("Student AUP") apply to all System activity. This policy is intended to clarify those expectations as they apply to computer and network usage and is consistent with Board Policy CQ (Local).

McKinney ISD believes that the access to information resources and opportunities for collaboration, when used in a responsible manner, will provide educational benefit for students and staff.

AVAILABILITY OF ACCESS

Access to the District's electronic communication and data management systems, including without limit, its telephone system, computer networks, electronic mail systems, videoconferencing systems, and its Internet and intranet access capabilities (referred to throughout as the "System"), shall be made available to students for identified educational purposes only.

Access to the System is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with Board Policies. Violations of law may result in prosecution as well as disciplinary action by the District.

System users may not gain unauthorized access to resources or information. Attempts to read, delete, copy, or modify the electronic mail of other System users, interference with the ability of other System users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited. Users must closely monitor their System passwords. Users should

protect their password(s) to help ensure the security and integrity of the System. In order to maintain the integrity of the System, users should not disclose their passwords to any other person. No user should attempt to gain access to another user's electronic mailbox, telephone voicemail box, computer files, or Internet account. Unauthorized access or attempts to access the System are strictly prohibited and will result in appropriate disciplinary action.

The loading of software to the System, including but not limited to, District managed hardware is considered a violation of the Student AUP.

Any attempt to harm or destroy the System, District equipment or data, the data of another user of the District's System, or the data of any of the agencies or other networks that are connected to the Internet, are prohibited. Violating the integrity of the District's System and/or data files or manipulating the District's System and/or data files without proper authorization is prohibited. Students are prohibited from bypassing the District filters and security protocols. Attempts to degrade or disrupt system performance are violations of Board Policy, the Student Code of Conduct, and the Student AUP and may constitute unlawful activity under applicable State and Federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses and "hacking" into the data or system of another user of the District's System, or any of the agencies or other networks that are connected to the Internet.

System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee, unless permitted by the doctrine of fair use.

The District reserves the right to use the District's System for purposes it sees fit and reserves the right to monitor all activity on the System, including individual student user accounts.

DISCLAIMER OF LIABILITY

The District shall not be liable for a student's inappropriate use of electronic communications resources or violations of copyright restrictions or other laws, a student's mistakes or negligence, and for any costs incurred by a student through use of the System. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet. No warranties of any kind are offered either expressed or implied.

STUDENT STANDARDS OF CONDUCT

All students are required to abide by the Student Code of Conduct, District Policy, State and Federal laws, and the Student AUP when communicating with others. This communication includes, without limit, communication with District employees or other students of the District, regardless of whether such communication occurs through use of the System. Additionally, students are responsible for following the Student Code of Conduct, District Policy, State and Federal laws, and the Student AUP when accessing the Internet through use of the System, while on campus, and while at school sponsored events. These same rules apply when using District sponsored websites, blogs, and Eduphoria. Furthermore, use of the District's System resources

to access external, non-District approved blogs, micro-blogs, chat rooms, messaging services, or social networking sites without first obtaining written permission from the designated campus administrator, is strictly prohibited. Social networking sites include, but are not limited to, Facebook, Twitter, Flickr, SnapChat and dating or match-making websites.

Students are required to follow the Student Code of Conduct and Board Policy regarding the use and possession of personal telecommunications devices on school property and at school sponsored functions. [*See* Board Policy FNCE (local)].

VIOLATIONS/SANCTIONS

Non-compliance with the Student AUP and/or District Policy may result in suspension of access, termination of privileges, and/or other disciplinary action consistent with Board Policies and State or Federal law. [*See* Board Policies FO series]. Additional disciplinary action may be determined at the building level in accordance with the Student Code of Conduct. Violations of law may result in referral to law enforcement as well as disciplinary action by the District. Persons whose violations of the Student AUP result in system disruption or damage may be responsible for reimbursement of costs incurred in system restoration.

MONITORED USE

Electronic mail transmissions and other use of the System by students are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use.

One level of security McKinney ISD has implemented is the installation of an Internet filtering service. Students may not disable, or attempt to disable, any Internet filtering service. In addition, all students will receive classroom instruction regarding appropriate technology use and acceptable Internet behavior, including a review of the Student AUP. System users and parents of students with access to the System should be aware that use of the System may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. McKinney ISD makes every effort to limit access to objectionable material; however, controlling all such materials on the Network/Internet is impossible, even with filtering in place. A student who gains access to such material is expected to discontinue the access as quickly as possible and to immediately report the incident to the supervising teacher or staff. Ultimately, however, it is the user's responsibility to appropriately use technology resources. Should a user be found in violation of the Student AUP, the incident will be regarded as a violation of with school rules and the Student Code of Conduct, resulting in disciplinary measures.

ACCEPTABLE USE

The District's System will only be used for learning, teaching, and administrative purposes consistent with the District's mission and goals. Commercial use of or solicitation using the District's System is strictly prohibited. The System may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District Policy or guidelines. Students will be provided information regarding appropriate online behavior, appropriate interaction with others on social networking sites and chat rooms, and cyber-bullying awareness and response in accordance with Board Policy CQ(LOCAL).

1. Responsibility:

- Student access to telecommunications and networked information resources shall follow guidelines developed for the selection of appropriate instructional materials contained in Board Policy EFA (Local)
- Since access could extend beyond evaluated or previewed resources, students and parents must be informed that inappropriate materials could be encountered during students' research required to achieve valid instructional objectives. If such inappropriate material is inadvertently encountered, it shall be disengaged from immediately.
- Users may not purposefully access materials or send or post messages, that are offensive, abusive, obscene, profane, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, racially offensive, or illegal. Students are expected to use appropriate language and refrain from swearing, using vulgarity, and/or ethnic or racial slurs.
- During school, teachers will help guide students toward appropriate materials. Outside of school, families bear responsibility for such guidance as they exercise with other information sources such as television, telephones, movies, radio and other potentially offensive media.
- While using the Internet on district computers, you may not give out your first name, last name, your picture, your parents' names, your telephone number, your address, or your Social Security number.
- Students should never use District equipment to make appointments to meet people whom they met on-line and should report to a teacher or administrator if they receive any request for such a meeting.

2. Privacy:

- Network storage areas may be treated like school lockers. Designated District staff may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on District servers or District approved Internet sites such as Google Drive, Canvas etc. will always be private.
- Any attempt to harm or destroy District equipment or data or the data of another user of the District's System, or any of the agencies or other networks that are connected to the Internet is prohibited. Violating the integrity of the District's data systems or manipulating the District's data files without proper authorization is prohibited. Attempts

to degrade or disrupt system performance are violations of Board Policy and administrative regulations and may constitute unlawful activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses and "hacking" into the data or system of another user of the District's System, or any of the agencies or other networks that are connected to the Internet.

COPPA NOTICE

The Children's Online Privacy Protection Act (COPPA) is a federal law governing the online collection of personal information from children under 13. The rules spell out what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online. McKinney ISD utilizes several educational software applications and web-based services that are operated by third parties. In order for our students to use these valuable programs and services, certain personal identifying information, generally the student's name and username and/or email address, must be provided to the website operator. Under federal law, these websites must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. The law permits schools to consent to the collection of personal information on behalf of all of its students, eliminating the need for individual parental consent given directly to the website operator. More information regarding COPPA is available on the Federal Trade Commission website at www.ftc.gov.

A list of applications and websites that may be used in District classrooms, with links to their privacy policies and terms of service, is available on the McKinney ISD website at www.mckinneyisd.net/departments/technology.

MCKINNEY ISD
TECHNOLOGY RESOURCES
ACCEPTABLE USE AGREEMENT

My child and I have read, understand, and will comply with the McKinney ISD Technology Resources Student Acceptable Use Policy. We understand that non-compliance with this policy may result in suspension of my child's access or termination of my child's privileges and other disciplinary action consistent with Board Policies and state law. [*See* the Student Code of Conduct, and Board Policies FN series, and FO series.] I realize that any of my child's actions that are violations of law may result in criminal prosecution as well as disciplinary action by the District. Any violation of this policy that results in system disruption or damage may result in the assignment of financial liability to my child or me. Furthermore, I consent to the release of my child's personal information for the purpose of accessing educational software applications and web-based services utilized by the District. I have been informed that I can access a list of applications and websites that may be used in District classrooms on the McKinney ISD website.

Student signature: _____ Date: _____

Parent/Guardian signature: _____ Date: _____

PLEASE SIGN THIS FORM AND TURN IT IN TO YOUR CAMPUS' FRONT OFFICE.