Employee Acceptable Use Policy (AUP)

Board Policy Links – CQ, DH, DIA, FB, FFH, and AUP

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 the McKinney Independent School District ("McKinney ISD" or "District"). 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 employees. The District has deployed a wide-area network that will allow staff and students to communicate with each other and will provide the staff and students with access to a multitude of instructional and administrative resources. This also places ethical responsibilities on all technology users.

Employees 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 for employee conduct apply to all System activity [*see* Board Policy DH series and this Technology Resources Employee Acceptable Use Policy ("Employee AUP")]. This policy is intended to clarify those expectations as they apply to computer and network usage and is consistent with Board Policy CQ (Local).

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 throughout as the "System"), shall be made available to employees primarily for educational and administrative purposes.

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.

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

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 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.

System users will immediately notify a campus administrator or Technology Services (informationsecurity@mckinneyisd.net) if a potential security problem is suspected or exists.

The district expects that all users will transmit information only in an appropriate and responsible manner. Any display or transmission of sexually explicit images, messages, or cartoons, or any use of the System that contains vulgarity, swearing, ethnic or racial slurs or epithets, or any material that might be construed as harassing or disparaging of others on the grounds of race, national origin, sex, age, religion, or disability violates the Employee AUP and is strictly prohibited.

System users should be mindful that use of school-related electronic mail addresses might result in some recipients or other readers of that mail to assume the System user represents the District or school, whether or not that was the user's intention.
System users may not attach program files to an e-mail message. "Spamming" and sending and/or forwarding unsolicited e-mails are prohibited. System Users may not use District electronic mail to promote activities or events for individuals or organizations not directly affiliated with, or sanctioned by, McKinney ISD. Commercial use of the District's System, including electronic mail, is prohibited. Users should be sure that all e-mail messages that are being sent are addressed only to the intended recipients. Use of the "Reply to All" feature in email should be used for normal email communications between a small group and NOT for campus wide or district wide emails.

System users may not gain unauthorized access to System and/or District resources or information. Unauthorized access or attempts to access the System are strictly prohibited and will result in appropriate disciplinary action.

Loading of software to the System, including but not limited to District managed hardware, is only allowed from the approved McKinney ISD Self Service Portal. Loading of any other software is considered a violation of the Employee AUP. Only District personnel, from Technology Services, are authorized to load additional software on the District's System.

System users are responsible for following Board policy, including but not limited to CQ Local and CQ Legal, and guidelines established in the Employee AUP at all times when using District owned equipment. The District retains all rights and ownership to all programs, data, materials, and electronic works created by District employees on, or using, the District System. Users of the System shall not send (upload) or receive (download) copyrighted materials, trade secrets, proprietary information, software programs, or similar materials except as authorized by the System administrator or designee. [See EFE (local) Instructional Resources: Copyrighted Material].

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.

All District data must be stored on District resources or District controlled services. District resources include, but are not limited to, District computers, District shared drives, "H" drives, and programs such as eSchoolPLUS, Munis, Laserfiche, and the Employee Portal. District controlled services include, but are not limited to, Google Drive, Microsoft Office 365 (OneDrive), and eSped, using a District provided account associated with the employee's District email. District data should never be stored on a personal computer, drive, or service associated with a personal account.

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. Attempts to degrade or disrupt system performance are violations of Board Policy, administrative regulations, and the Employee 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.

Forgery or attempted forgery of electronic mail messages or misrepresentation of the identity of a sender is prohibited. 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.

Information transmitted via the System is considered confidential District information and may not be disclosed to persons other than the intended recipient without prior authorization. Users must closely monitor their System passwords. Users should protect their password(s) to help ensure the security and integrity of the System. 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 unless expressly authorized to do so, by an authorized representative of the District. Any user who receives information such as electronic mail messages in error should not read the message and delete immediately.

Data Privacy and Protection

Employees have a responsibility to protect the "personally identifiable information" (PII) and confidential data of any student, guardian, or employee information that they have access to. PII and confidential information includes, but is not limited to, name, social security number, driver's license or state ID number, medical information, date of birth, economic status, discipline infractions, race or ethnic information, academic or job performance, and home address.

The following requirements must be followed to protect the PII and confidential data entrusted to the district:

1. PII/photos of McKinney ISD students will not be posted on the MISD websites other than as permitted under District Processes/Guidelines and State and Federal law.
2. PII will not be loaded or sent to third party systems/software without district approval.
3. Email is not considered a secure method of transmission. PII other than name, email, and phone number will not be included in the subject or body of an email sent outside of the District. PII or confidential data may be included in an **encrypted** attachment provided the password is not included in the email.
4. PII or confidential data stored on systems or services that allow sharing, including Google Drive and Microsoft OneDrive, must be secured by employees and shared with only those school officials who have a legitimate educational interest in the data. PII or confidential data should never be shared publicly or broadly within an entire school or the entire District.

To the extent employees' access student records and/or information through the System, employees must only access those records to which they are entitled to access as a school official with a legitimate educational interest in the records. In accordance with McKinney ISD Board of Trustees' Policies FL (LEGAL) and FL (LOCAL), "school officials" include:

1. An employee, trustee, or agent of the District, including an attorney, a consultant, contractor, a volunteer, and any outside service provider used by the District to perform institutional services.
2. An employee of a cooperative of which the District is a member or of a facility with which the District contracts for placement of students with disabilities.
3. A contractor retained by a cooperative of which the District is a member or by a facility with which the District contracts for placement of students with disabilities.
4. A parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

A school official has a "legitimate educational interest" in a student's record when he or she is:

1. Working with the student;
2. Considering disciplinary or academic actions, the student's case, or an individualized education program for a student with disabilities;
3. Compiling statistical data;
4. Reviewing an education record to fulfill the official's professional responsibility; or
5. Investigating or evaluating programs.

Employees violate this policy if they access information in which they do not have a legitimate educational interest, as defined above (e.g. accessing information of student's not in the employee's class, not on the employee's campus, etc.).

Monitored Use

For security and network maintenance purposes, authorized individuals within McKinney ISD may monitor equipment, systems, and network traffic at any time. Electronic mail transmissions and other use of the System by employees are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use.

The System's software and hardware that provides the District email capabilities has been publicly funded. For that reason, use of the System should not be considered a private form of communication. The content of any communication of this type is governed by the Open Records Act and the District is required to abide and cooperate with any legal request for access to email contents by the proper authorities.

One level of security McKinney ISD has implemented is the installation of the Internet Filtering Service. Employees that have an instructional need to access web sites that may be blocked should submit a ticket through the district help desk. In addition, all employees will receive classroom instruction regarding appropriate technology uses and acceptable Internet behavior, including a review of the Employee AUP. It is the user's responsibility to appropriately use technology resources. Should a user be found in violation of this policy, the incident will be regarded as a violation of school rules and Board Policy, resulting in disciplinary measures.

Records Retention

In accordance with the District's record management program, employees shall retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources. Please be aware that electronic mail stored in user created folders on the District server will remain for five (5) years (email remaining in the user's inbox will be deleted after 90 days). Employees shall keep all work-related electronic mail on the server and not archived elsewhere to a location off the server.

The District shall preserve documents, including electronically stored information, and suspend routine record destruction practices as applicable according to procedures developed by the records management officer:

1. In the event of pending or reasonably anticipated litigation;
2. In the event of an investigation by a federal agency or department or any bankruptcy case; or
3. In the event of a public information request.

Notification shall be given to appropriate staff of any applicable obligations to suspend routine record

destruction practices. [See Board Policy CQ (local) and CPC (local)]

All District employees are required to abide by the Code of Ethics and Standard Practices for Texas Educators ("Code of Ethics"), State and Federal law, District Policy, this Employee AUP, and ethical standards when communicating with students and other employees, regardless of whether such communication takes place on campus, during instructional time, through use of the System, or not. District employees shall recognize these laws and regulations apply to any and all communication with students and other employees, including, but not limited to, use of email, social networking sites, cell phones, and text messaging.

Electronic Communication

System users will ethically use electronic communication including telephone, cellular telephone, computer, computer network, personal data assistant or a pager. Communication includes emails, text messages, instant messages and any communication used through Internet websites including social media websites or social networking websites. All confidential data contained within an email message or attachment must be secured.

Ethical Use

Additionally, the Code of Ethics, Standard 3.6 provides, "the educator shall not solicit or engage in sexual conduct or a romantic relationship with a student." [*See* Board Policy DH (exhibit)]. Educators shall maintain the proper decorum in any and all communication with students, regardless of whether such communication occurs during or outside of the instructional day.

In accordance with McKinney ISD's expectations, District employees are prohibited from posting any information, pictures or otherwise, on the Internet that results in a violation of the Code of Ethics, State and Federal law, and District Policy, including the District's Standards of Conduct for all employees. District employees are also prohibited from using the District's System to access sites in violation of this Employee AUP, as detailed above (see section titled "Acceptable Use"). Please be aware that the District will hold employees responsible for any and all information deemed objectionable by the Code of Ethics, State and Federal law, District Policy, or this Employee AUP on an Internet site that is within the control of an employee, including, but not limited to, comments sent from third parties to the employee's site. District employees are required to abide by the Code of Ethics as defined in Board Policy DH (exhibit), when accessing all Internet sites, including blogging sites, micro-blogs, chat and messaging services, and social networking sites. Social networking sites include, but are not limited to Facebook, Twitter, Flickr, and dating or match making websites. District employees, who use social networking sites as a means of communication with students outside of their capacity as an educator or District employee, shall ensure that all communications with students or other employees are consistent with the District's Standards of Conduct, the Code of Ethics, State and Federal law, District Policy, and this Employee AUP.

The District recognizes and respects an employee's right to freedom of speech. [See Board Policy DG (legal)]. However, when the right impinges on, and/or compromises, an employee's ability to effectively perform his/her work, the District must take appropriate action. Specifically, the District will investigate and, when necessary, evaluate disciplinary action when information posted by an employee on an Internet site results in conduct including, but not limited to: conduct that compromises the dignity of the profession; conduct that does not respect and obey the law; conduct that does not demonstrate integrity; conduct that does not exemplify honesty; conduct that constitutes moral turpitude; or any other conduct in violation of Board Policies. [See Board Policies DH series].
Accessing and/or modifying such sites utilizing the System may also result in a violation of the Employee AUP.

Violation/Sanctions

Non-compliance with the Employee 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* the Employee Handbook and Board Policies DH series]. Violations of law may result in criminal prosecution as well as disciplinary action by the District. Persons whose violations of the Employee AUP result in system disruption or damage may be responsible for reimbursement of costs incurred in system restoration.

Disclaimer of Liability

The District shall not be liable for an employee's inappropriate use of electronic communications resources or violations of copyright restrictions or other laws, an employee's mistakes or negligence, and for any costs incurred by employees through the 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.