Katy Independent School District

Staff Responsible Use Guidelines for Technology

Katy Independent School District makes a variety of communications and information technologies available to District staff through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have significant consequences, harming the District, its students and its staff. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District staff and setting standards which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review. To educate District staff on proper computer/network/Internet use and conduct, users are required to review these guidelines at the beginning of each school year. All District staff shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. These guidelines are included in the District's Employee Handbook. "Staff" shall be used in this document to refer to all District employees.

Definition of District Technology System. The District's computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Fax machines;
- Copiers;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, tools (Internet or District server based);
- District-provided Internet access;
- District-filtered public Wi-Fi;
- Virtual environments; and
- New technologies as they become available.

Availability of Access

Acceptable Use. Computer/Network/Internet access will be used to improve teaching and enhance learning consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/network/Internet use by all District staff.

Privilege. Access to the District's computer/network/Internet is a privilege, not a right.

Access to Computer/Network/Internet. Computer/Network/Internet access is provided to all District staff. All students will have access to the Internet unless parents request in writing that access be denied.

Access to the District's electronic communications system, including the Internet, shall be made available to staff primarily for instructional and administrative purposes and in accordance with administrative regulations. Each District computer and public Wi-Fi (available for individuals who bring their own personal telecommunication devices) has filtering software that blocks access to visual depictions and/or content that are obscene, pornographic, inappropriate, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA.

Limited personal use is permitted if the use imposes no tangible cost to the District, does not unduly burden the District's computer or network resources, and has no adverse affect on a staff member's job performance.

All nonstaff/nonstudent users must obtain approval from the principal or departmental supervisor or designee to gain individual access to the District's system.

All individual staff users of the District's system must complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or departmental supervisor's office.

Staff are required to maintain password confidentiality by not sharing their password with others and may not use another person's system account.

Staff identified as a security risk or having violated the District's Staff Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

Content/Third-Party Supplied Information. Staff with access to the District's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material.

Staff who knowingly bring prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Subject to Monitoring. All District computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Staff should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Staff should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose. Personal telecommunication devices are subject to examination in accordance with these guidelines.

Use of Personal Telecommunication Devices. The District will provide a filtered, wireless public network to which staff will be able to connect personal telecommunication devices for instructional and administrative functions. These devices are the sole responsibility of the staff owner. The campus or District assumes no responsibility for personal telecommunication devices if they are lost, loaned, damaged or stolen and only limited time or resources will be spent trying to locate stolen or lost items. Each staff member is responsible for their own device; set up, maintenance, charging and security. District staff will not diagnose, repair or install software on another staff member's or student's device. Should inappropriate activities or a security breach be detected, appropriate District staff may examine the staff member's device.

Staff Computer/Network/Internet Responsibilities

Staff are responsible for their actions in accessing available resources.

District staff are bound by all portions of the District's Staff Responsible Use Guidelines. Staff who knowingly violate any portion of the Staff Responsible Use Guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Campus- and Departmental-Level Responsibilities. The principal/departmental administrator or designee will:

1. Be responsible for disseminating and enforcing the District's Staff and Student Responsible Use Guidelines at the campus or departmental level.

2. Ensure that all staff users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or departmental supervisor's office.
3. Ensure that staff supervising students who use the District's systems provide information emphasizing its appropriate, safe, and ethical use.
4. Monitor all users of the District's systems to ensure appropriate and ethical use.
5. Use the District's student management system to identify students who do not have permission to use the Internet and inform staff who are responsible for these students that they do not have permission to use the Internet, student email or Websites that require parental consent for students under the age of 13.
6. Provide training to staff that supervise students on digital responsibility, digital citizenship/ and appropriate use of technology resources.

Teacher Responsibilities. The teacher will:

1. Provide age-appropriate lessons in Internet safety, digital responsibility, and cyber security for students throughout the year.
2. Review District computer/network/Internet responsibilities prior to gaining access to such system.
3. Make parents aware of the District informational Web 2.0 page.
4. Verify the list of students (age 13 and younger) who require additional parent consent to access the Internet, email, and Websites through the reporting feature in the student management system.
5. Provide developmentally-appropriate guidance to students as they use electronic resources related to instructional goals.
6. Use computer/network/Internet in support of instructional goals.
7. Provide alternate activities for students who do not have permission to use the Internet or email.
8. Provide a variety of comparable activities for students who do not bring their own device.
9. Address student violations of the District's Student Responsible Use Guidelines as defined in the *Discipline Management Plan and Student Code of Conduct*.

Katy ISD Staff Code of Conduct. District staff are expected to maintain appropriate conduct when accessing the communications and information technologies available through computer/network/ Internet access. All staff must comply with the District's Staff Responsible Use Guidelines at all times when accessing any part of the technology system.

Staff will guard and protect access to secure systems by:

1. **Protecting passwords and other similar authorization information.** Passwords are the primary way in which staff members are authenticated and allowed to use the District's computing resources. Staff will not disclose personal password(s) to any individual, including another staff member. Similarly, staff will not disclose other identifying information used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.
2. **Guarding unauthorized use of resources.** Staff will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied.
3. **Not circumventing or compromising security.** Staff must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the District's systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and intentional transmission of viruses or worms.

Computer/Network/Internet usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the District for any purpose. Staff will affirm, in writing, that at all times their actions while using the District's system will not violate the law or the rules of network etiquette, will conform to the guidelines set forth in the Staff Responsible Use Guidelines, and will not violate or hamper the integrity or security of the District's technology system.

If a violation of the Staff Responsible Use Guidelines occurs, staff will be subject to one or more of the following actions:

1. Revocation of access;
2. Disciplinary action;
3. Loss of employment with the District; and/or
4. Appropriate legal action.

Use of Social Networking/Digital Tools. Staff may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions.

The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools. Staff who use digital learning tools in their classrooms must monitor student actions to ensure compliance with the *Discipline Management Plan and Student Code of Conduct*.

Use of System Resources. Staff are asked to purge email or outdated files on a regular basis.

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the staff should immediately notify the District's Help Desk. The security problem should not be shared with others.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses and are prohibited:

Violations of Law. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- threatening, harassing, defamatory or obscene material;
- copyrighted material;
- plagiarized material;
- material protected by trade secret; or
- blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws.

Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the litigation process.

Modification of Computer. Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Transmitting Confidential Information. Staff may not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information about oneself such as, but not limited to, home addresses, phone numbers, email addresses, birthdates of or of others is prohibited.

Commercial Use. Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-KISD Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief. Any malicious attempt to harm or destroy District equipment, materials or data; or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. Staff committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See DH in Board Policy.]

Copyright. Staff must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

Copyright Violations. Downloading or using copyrighted information without following approved District procedures is prohibited.

Intellectual Property. An original work created by a student that will be published on the Internet will require written parental consent.

Plagiarism. Fraudulently altering or copying documents or files authored by another individual is prohibited.

Impersonation. Attempts to log on to the computer/network/Internet impersonating a system administrator or District staff, student, or individual other than oneself, will result in revocation of the staff member's access to computer/network/Internet.

Illegally Accessing or Hacking Violations. Intentional or unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

System Interference/Alteration. Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Email and Communication Tools

Email and other digital tools such as, but not limited to blogs and wikis, are tools used to communicate within the District. The use of these communication tools should be limited to instructional, school-related activities, or administrative needs.

Staff will be issued email accounts. Staff should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations. Email attachments, both internal and external, are limited to 30MB or smaller.

Staff should keep the following points in mind:

Perceived Representation. Using school-related email addresses, blogs, wikis, and other communication tools might cause some recipients or other readers of the email to assume that the staff member's comments represent the District or school, whether or not that was the staff member's intention.

The Katy ISD email account should be used for professional communication. The social media tools that are associated with the District's email account should be for professional use. For example, an employee must not associate their Katy ISD email account with a personal Facebook account. However, the Katy ISD email account must be used if the Facebook account or Edmodo account was intended for professional purposes.

Privacy. Email, blogs, wikis, and other communication within these tools should not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, should not be divulged. To avoid disclosing email addresses that are protected, all email communications to multiple recipients should be sent using the blind carbon copy (bcc) feature, if applicable.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Communications with Students. As specified in the Employee Standards of Conduct [Board Policy DH (EXHIBIT)], **employees shall refrain from inappropriate communication with a student or minor, including, but not limited to, electronic communication such as cell phone, text messaging, email, instant messaging, blogging, or other social network communication. The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity). Factors that may be considered in assessing whether the communication is inappropriate include, but are not limited to:**

- **The nature, purpose, timing, and amount of the communication;**
- **The subject matter of the communication;**
- **Whether the communication was made openly or the educator attempted to conceal the communication;**
- **Whether the communication could be reasonably interpreted as soliciting sexual contact or a romantic relationship;**
- **Whether the communication was sexually explicit; and**
- **Whether the communication involved discussion(s) of the physical or sexual attractiveness or the sexual history, activities, preferences, or fantasies of either the educator or the student.**

The employee does not have a right to privacy with respect to communications with students and parents.

The employee continues to be subject to federal laws, local policies, and administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, including:

- Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records.
- Copyright law
- Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.

Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.

Political Lobbying. Consistent with State ethics laws, District resources and equipment, including, but not limited to, emails, blogs, wikis, or other communication tools must not be used to conduct any political activities, including political advertising or lobbying. This includes using District email, blogs, wikis, or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails, blogs, or wikis regarding any political advertising.

Forgery. Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

Junk Mail/Chain Letters. Generally staff should refrain from forwarding emails which do not relate to the educational purposes of the District. Chain letters or other email intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

eNews Regulations

The eNews system is designed to supplement communications between the District and/or campus and parents. It is to be utilized for one-way communication with parents/guardians regarding District- and campus-specific news only.

Guidelines for eNews System Management

1. Usage of the eNews system should be available for both campus administrators and school-affiliated parent organizations.
2. eNews should be utilized as one component of a campus-parent communications plan, not a replacement for other communication tools.
3. eNews may only be sent to email addresses of parents/guardians, staff or eNews subscribers.
4. A student's name may be included in eNews messages as long as the student's directory information privacy code allows for the release of this information ("A" code only) or if special permission is obtained from the parents of a student with an "O" or "N" code. Other student directory information, such as photographs, address and phone number, should not be included in an eNews message.
5. eNews may not be used for solicitations from outside organizations or vendors.
6. The District's Communications Department shall be responsible for composing, editing and distributing all District eNews messages. District eNews messages must be approved by the Director of Communications or his/her designee prior to distribution.
7. The campus principal shall designate an eNews coordinator whose duties shall include gathering proposed messages and editing them for content and compliance with all District privacy guidelines for campus eNews. All campus eNews must be approved by the campus principal prior to being distributed to parents/guardians.

District Web Contributor Responsibilities

The purpose of District Web sites is to communicate campus, department, and District activities and information to District Web patrons and staff. Official school and District Web sites should be hosted on a District Web server. All staff creating/editing content for display on District Web servers are considered District Web-content contributors.

In conjunction with the District's Technology Department, the District's Communications Department is responsible for ensuring that all Web-site contents, including but not limited to katyisd.org, campus Webs and teacher Webs, conform to the guidelines described below, as well the District's overall communications objectives. As such, the Communications Department reserves the right to alter or delete any content contained on a District Web site in order to ensure that it conforms with both Web-site guidelines and the District's communications objectives.

Content Issues

For the requirements below, "content" is defined as text, graphics, media, or other information that is visible and/or audible on a District Web page.

- All content must be approved by principals/department heads or their designees before being posted to District Web servers.
- If any content and/or file [that is saved on a District Web server or content on an external (non-District ISD) Web site to which a hyperlink from a District Web page refers] exhibits any of the following conditions or presents any of the following problems, the individual responsible for that content will be asked to eliminate the offending condition within a reasonable amount of time. If the condition is not corrected after a reasonable amount of time, the District's Technology Department will take action to rectify the situation. Staff who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

  Content shall not be displayed if it:

  - ❖ Contains questionable and/or inappropriate material and/or themes.
  - ❖ Is of a personal nature.
  - ❖ Includes commercial, trademarked, and/or copyrighted material without the express written consent of the "owner" of the content. If consent is obtained, the proper trademark/copyright symbol and/or owner's credits must be displayed.
  - ❖ Is out-of-date or inaccurate.
  - ❖ Contains hyperlinks that do not return an active Web page and displays a "Page Not Found".
  - ❖ Contains hyperlinks that do not return a document and displays a "Page Not Found".
- Staff should only use Web sites on District Web servers to post class information; however, staff are allowed to post information related to curriculum projects using District-approved blog and wiki sites.
- Personal information about District staff and/or parent volunteers will not be disclosed without the approval of the individual and the principal/administrator and will be in accordance with District/campus procedures. Non-District email addresses, non-District mailing addresses, and non-District phone numbers will not be disclosed on District/campus Web sites.
- Pictures and names of staff and/or parent volunteers are allowed with their written approval.

Display of Student Information on the Internet

The following conditions apply to the display of student information on District Web sites. A content contributor who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

- Student-created projects, writings, and/or artwork are permitted on campus/District Web sites, or District-approved blog and wiki sites, if the appropriate parental consent has been obtained.
- Student photographs and names are permitted if the directory information privacy code specified for the student allows for it (code "A" only).
- For a student with an "N" or "O" directory information privacy code, specific parental consent must be obtained to display each photograph of the student.
- The "Digital Responsibility" mandatory training will provide guidance in the best practices for displaying student's work on the Internet.

Hyperlinks

The following requirements must be met to utilize hyperlinks on any District Web page. If these conditions are not met, the individual responsible for those hyperlinks will be asked to eliminate the offending condition within a reasonable amount of time, after which the District's Technology Department will take action to rectify the situation. If the condition is a violation of (or promotes the violation of) any District policy or regulation or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content and/or file may be recommended.

- Hyperlinks to external (non-District) Web sites must include the following text on the District Web page where the hyperlink exists: "Katy ISD is not responsible for content on external sites or servers."

- Hyperlinks to all external (non-District) Web sites must open those Web sites in a new window.
- Hyperlinks to external (non-District) Web sites are only allowed where the content in those Web sites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide service to District Web patrons. However, if the content in these Web sites is judged unsuitable at any time, the hyperlink to the site will be removed.
- Hyperlinks to Web sites, whose content is prohibited by the District's Web filtering system, will not be allowed.
- Hyperlinks to District staff or volunteer personal Web sites are not allowed.
- Hyperlinks to personal student Web sites are prohibited.

Email Links
District email addresses (those email addresses ending with "@katyisd.org") will not be displayed on District public Web sites without being linked to a **District email Web form**. If an email address is using the traditional "mail to" html code, the individual responsible for that email link will be asked to revise his/her code in a reasonable amount of time, after which, the situation will be rectified by the District's Technology Department. Email links can be displayed in one of these two methods:

1. If the email link is being displayed in a Katy Web, one must use a Web control specifically provided to display contact information including the contact's email address.
2. If an email link is being displayed in a District's Web site other than a Katy Web, one must utilize code that invokes the email Web form. Upon request, this code will be provided to the individual desiring to display an email link.

Special Features
There are special Web-site features that will not be allowed on District Web sites.

- No executable programs or applets are allowed on District Web sites.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the staff member's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary action and/or appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to sites that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the staff member's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.