TECHNOLOGY ACCEPTABLE USE GUIDELINES AND USER AGREEMENT

Introduction

The Kettle Moraine School District (District) provides students, staff, agents, guests, and volunteers, collectively known as “user” or “users” for educational and business purposes, with access to Information Technology and Communication Resources to accomplish its mission of educating students in conformance with applicable law.

A user is deemed to access and use the system through any electronic activity conducted on the system using any device (whether or not such device is a District provided device) regardless of the user’s physical location.

“Information Technology and Communication Resources” (system) refers to Internet connections (including wireless connections), e-mail accounts, intranet, any remote connection to District systems, telephones (including cell phones and the voicemail system), computers (whether used on or off campus), fax machines, digital communications (including email), wireless access points, printers, cameras, removable storage devices, and any other device or equipment that the District reasonably deems to fall within the scope of these Guidelines. By using the District’s system, users agree to abide by the Guidelines set forth in this agreement and all other District guidelines, policies, procedures, rules, and regulations. All staff and students are required to have a signed agreement form on file.

Privacy and Monitoring

Users of the system shall have no expectation of privacy with respect to such use. Consequently, all software, email, voicemail, files, digital communications, and other information or documents used, generated, transmitted or received over District data, voice or video networks, or stored on District equipment, are the property of the District. The District retains the right to review, monitor, audit, intercept, access and disclose all messages or information created, received or sent over District data, voice or video networks, or stored on its equipment. External electronic storage devices are subject to monitoring if used with District resources. Additionally, email messages, text messages, and other documents created or received by staff may be subject to release in accordance with applicable public records law.

General Use

Information Technology and Communication Resources provided by the district are intended for educational use, instruction, research and the facilitation of communication, collaboration, and other District-related purposes. Users are subject to the same standards expected in a classroom and/or professional workplace. The District reserves the right to prioritize use and access to the system. The ultimate responsibility for acceptable use is the sole responsibility of the individual user.

Diligent effort must be made to conserve system resources. No person shall have access to the system without having a signed **Technology Acceptable Use Guidelines & User Agreement** on file with the District. Nothing in these Guidelines is intended to preclude the supervised use of the system while under the direction of a teacher or other approved user acting in conformity with District policy and procedure nor is it intended, where appropriate, to prohibit communication of union business as defined under the Negotiated Agreement with unionized personnel.

System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account information or password with another person or leave an open file or session unattended or unsupervised. Users are ultimately responsible for all activity under their account. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, misrepresent other users on the system, or attempt to gain unauthorized access to the system. Communications may not be encrypted so as to avoid security review. Users should change passwords regularly and avoid easily guessed passwords.

Examples of Acceptable Use

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.

- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

Examples of Unacceptable Use

Users may not engage in any of the activities prohibited by these Guidelines when using or accessing the District's system. If a user is uncertain whether behavior is prohibited, he or she should contact a teacher, supervisor or other appropriate District personnel. The District reserves the right to take immediate action regarding activities that (1) create security and/or safety issues for the District, students, employees, schools, network or computer resources, or (2) expend District resources on content the District determines lacks legitimate educational or District content or purpose, or (3) the District determines are inappropriate.
I will not:

- Use school technologies in a way that could be personally or physically harmful to myself, others, or District property.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others–staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Download, post, reproduce or distribute music, photographs, video or other works in violation of applicable copyright laws.
- Plagiarize content I find online.
- Post personally-identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts, or content that isn't intended for my use.
- Use the District system for commercial purposes or for personal financial gain.
- Use the District's system on behalf of any elected official, candidate, candidates, slate of candidates or a political organization or committee.
- Engage in criminal or other unlawful activities.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Personally-Owned Devices

Students may use personally-owned devices (including laptops, tablets, smartphones, and cell phones) as allowed by building policy—unless such use interferes with the delivery of instruction by a teacher or staff or creates a disturbance in the educational environment. Any misuse of personally-owned devices may result in disciplinary action. Therefore, proper netiquette and adherence to the acceptable use policy should always be used. In some cases, a separate network may be provided for personally-owned devices.

Digital Citizenship / Social Media Guidelines

Recognizing that collaboration is essential to education, KMSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Digital citizens respect and protect themselves, others, and intellectual property online; as such, users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online (see Protection of Personally Identifiable Information below).

Filtering

In accordance to Children's Internet Protection Act ("CIPA"), the District blocks or filters content over the Internet that the District considers inappropriate for minors. This includes pornography, obscene material, and other material that may be harmful to minors. The District may also block or filter other content deemed to be inappropriate, lacking educational or work-related content, or that pose a threat to the network. The District may, in its discretion, disable such filtering for certain users for bona-fide research or other lawful educational or business purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities. Additional information regarding CIPA can be found here: http://fcc.us/174NFg5

Cyberbullying

Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, outing, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Protection of Personally Identifiable Information

The Family Educational Rights and Privacy Act ("FERPA") prohibits District school officials from disclosing personally identifiable information ("PII") from education records of District students and families to third parties without parental consent. All users of the District's system must comply with FERPA. Users should ensure that communications that include or attach confidential information are only sent to the intended recipients.

Personal information such as home and school addresses, telephone numbers and full name should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other adult. Students should never make appointments to meet people in person that they have contacted on the system without District and parent permission. Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

Google Apps for Education and Online Academic Services

All staff and students (collectively "user" or "users") will be assigned a Kettle Moraine School District (KMSD) Google Apps for Education account and will be accessing other Online Academic Service(s). A KMSD Google Apps for Education account allows staff and students to use Google Mail, Google Docs, and other Google applications and products for collaboration, communication, research and sharing. Online Academic Services include, but are not limited to, Google Apps for Education, Moodle, web-based math and literacy assessment software, skill-building games, content-focused video tutorials, and all other online digital resources. KMSD cannot and does not guarantee the security of electronic files located on Google systems or any other Online Academic Service system. It is the responsibility of the user to backup important documents or files. KMSD cannot assure that users will not be exposed to unsolicited information.

Electronic Communications

Electronic communications are protected by the same laws and policies and are subject to the same limitations as other types of media. When creating, using or storing messages on the system, the user should consider both the personal ramifications and the impact on the District should the messages be disclosed or released to other parties. Extreme caution should be used when committing confidential information to the electronic messages, as confidentiality cannot be guaranteed. All electronic communications are subject to monitoring (see Privacy and Monitoring above).

The District archives all non-spam emails sent and/or received on the system in accordance with the *Wisconsin Records Retention Schedule for School Districts*. After the set time has elapsed, email communications may be discarded unless the records may be relevant to any pending litigation, pending public records request, or other good cause exists for retaining email records.

Users shall not electronically record by audio, video, or other means, any conversations or meetings unless each and every person present has been notified and consents to being electronically recorded. Persons wishing to record a meeting must obtain consent from anyone arriving late to any such meeting. Users shall not electronically record telephone conversations unless all persons participating in the telephone conversation have consented to be electronically recorded. These provisions are not intended to limit or restrict electronic recording of publicly posted Board meetings, grievance hearings, and any other Board sanctioned meeting recorded in accordance with District policy. These provisions are not intended to limit or restrict electronic recordings involving authorized investigations conducted by District personnel, or authorized agents of the District, or electronic recordings that are authorized by the District, e.g. surveillance videos, extracurricular activities, voicemail recordings.

Limitation of Liability

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed 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 warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data stored on or transmitted through the system or interruptions of service. The District will not be responsible for financial obligations arising through the unauthorized use of the system. 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 individual or entity 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 system.

From time to time, the District will make a determination on whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances non-student or non-staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the District. For security and administrative purposes the District reserves the right for authorized personnel to review system use and file content. The District reserves the right to remove a user account on the system to prevent further unauthorized activity.