Rich Township High School District 227
ACCEPTABLE USE OF TECHNOLOGY POLICY (AUP)

Approved July 21, 2015

Purpose

The purposes of the Acceptable Use of Technology Policy (AUP) are:

- **Section I:** For all students, employees, and other "users" of the School District's "electronic resources," as those terms are defined in this AUP, defining authorized access to and acceptable use of the District's electronic resources; mitigating the risk of disclosure or unauthorized access to private and protected information through the District's electronic resources; and complying with requirements of federal laws protecting student's use of electronic resources in public schools.
- **Section II:** For all students, defining authorized use of personal technology in "bring your own device" (BYOD) or "bring your own technology" (BYOT) programs, as those terms are defined in this AUP.
- **Section III:** For all employees, defining authorized use of personal technology to conduct "District business," as that term is defined in this AUP, including in BYOD or BYOT programs.
- **Section IV:** For all students, defining authorized use of technology for personal purposes on District property and at related events and activities.
- **Section V:** For all employees, defining authorized use of technology for personal purposes on District property, at related events and activities, and with "members of the District community," as that term is defined in this AUP.
- **Section VI:** For all employees and students, defining the terms under which official District Internet and social media websites may be operated and when one may operate an Internet or social media website to conduct District business or for educational or extra-curricular purposes.
- **Section VII:** Outlining the consequences of violating of the AUP.
- **Section VIII:** Setting forth requirements regarding notification and acknowledgement of the AUP by students, employees, and users of the District's electronic resources.

Administrative Procedures

The Superintendent or designee shall create administrative procedures implementing this policy, which, along with handbooks and guidelines issued at the school or department level, may supplement this policy.

Definitions

"Bring your own device (BYOD) or bring your own technology (BYOT) program": Programs under which students and/or employees are authorized to use personal technology devices not owned or licensed by the District, including personal computers, cell phones, and smart phones, for certain educational, extra-curricular, and/or business purposes identified in the program.

"District business": Any work conducted as an employee of the District, whether for educational, extra-curricular, or other business or operational purposes of the District. This includes communications with members of the District community in which the employee conducts or performs such work. District business might relate to education, instruction, student and employee relations and discipline, extra-curricular activities, professional activities, and other District operations. "District business" does not include protected concerted union activity.

"on District property or at related events and activities": Use is considered to be on District property or at a related event or activity when it occurs on, or within sight of, school grounds at any time, including before, during, and after school hours; off school grounds at a school-sponsored activity or event, or any activity or event that bears a reasonable relationship to school; and when traveling to or from school or a school activity, function, or event through District-sponsored transportation. Simply because use does not occur on District property or at a related event or activity does not mean the use is not subject to this AUP or other District policies and procedures, including discipline policies and procedures. For example, student or employee misconduct on technology may lead to consequences under this AUP or other District policies and procedures if the conduct materially and substantially interferes with, disrupts, or adversely affects the school environment, school operations, or an educational function, including conduct that may reasonably be considered to: (a) be a threat or an attempted intimidation of an employee; or (b) endanger the health or safety of students, employees, or school property, regardless of when or where that misconduct occurs.

"Electronic resources": The District's "electronic resources" include, but are not limited to, the District's electronic networks and information systems, such as the Internet, Wi-Fi, electronic data networks, and infrastructure for oral, visual, and written electronic communication, including electronic mail, text messaging, instant messaging, and chat programs. "Electronic resources" also include technology owned or licensed by the District and provided by the District for use by its employees or students, including, if offered, technology issued to students and/or employees (i.e., a "one-to-one" program), and District and District-authorized webpages and social media or websites. If a user accesses the District's electronic resources, including Internet service or Wi-Fi, with a personal technology device, that use is also considered use of "electronic resources" that is covered by this AUP.

"Includes" or "Including": When used in this AUP and any related administrative procedures, handbooks, and guidelines implementing this AUP, "includes" means "includes, but not limited to" and "including" means "including, but not limited to" and reference a non-exhaustive list.

"Internet publications": Webpages that are limited to the provision of information, allowing users to view content but not to contribute to the content of the webpage.

"Members of the District community": Students, parents, residents, employees, contractors and volunteers of the District, and other individuals serving, served by, and/or working with or for the District.

"One-to-one program": Program through which the District issues all students and/or employees, or certain groups of students and/or employees, District-owned or -licensed personal technological devices, such as personal computers and laptop computers, for educational, extra-curricular and/or business purposes identified in the program. The participant in the one-to-one program typically may take the technological device with them when they leave school grounds for use outside of normal school or business hours.

"Personal purposes": Any uses other than uses for "District business," such as accessing personal cell or smart phones, email, and social media websites such as Twitter, Facebook, and others for purposes other than District business. "Personal purposes" includes protected concerted union activity.

"Personal technology": All technology that is not owned or licensed by the District.

"Protected concerted union activity": Actions by employees concerning wages or working conditions, such as discussing work-related issues or terms and conditions of employment between employees or with members of the District community.

"Social media websites": Webpages that do not simply provide information, but rather allow users to comment, exchange or share content, collaborate, and/or interact. Also known as social networking websites. Examples of social media websites include Internet forums, weblogs (or "blogs"), video logs (or "vlogs"), wikis, social networks (such as Facebook, Twitter, and MySpace), podcasts, photograph and video sharing programs (such as YouTube and Instagram), rating websites, music-sharing websites, and crowdsourcing.

"Technology": Includes desktop computers, laptop computers, tablet computers, cell phones and smart phones, text messaging services, instant messaging services, and other technology, as well as any webpages or social media profiles, such as Internet forums, weblogs (or "blogs"), video logs (or "vlogs"), wikis, social networks and social media pages (such as Facebook, Twitter, and MySpace), podcasts, photograph and video sharing programs (such as YouTube and Instagram), rating websites, music-sharing websites, and crowdsourcing.

"User": A user of the District's electronic resources is any person who uses the District's electronic resources, with or without District authorization, and may include students, parents, employees, contractors, and volunteers of the District.

Section I: Acceptable Use of the District's Electronic Resources

Applicability

This section applies to all "users" of the District's electronic resources, including students and employees.

Acceptable Use – General

Only authorized users may access the District's electronic resources. This includes connecting personal technology devices to the District's electronic resources, including the Internet and Wi-Fi.

Access to the District's electronic resources is intended for educational and extra-curricular purposes and District business. Employees may use District electronic resources for incidental personal use during non-work times as long as that use complies with the other parameters of this AUP and any implementing procedures and does not interfere with the employee's job duties or the provision of education and services by the District. Students may only use the District's electronic resources for incidental personal use during non-instructional times if the student is authorized to use the particular electronic resource at the time used, the use complies with the other parameters of this AUP and any implementing procedures, and the use does not violate any other District policy or state or federal law.

Users must take reasonable steps to protect the security of the District's electronic resources. Among other things, users may not share passwords or allow others to access electronic resources using the user's password or profile. Any user who becomes aware of a security breach must notify a District representative immediately.

Users are responsible for appropriately using the District's electronic resources. If a user has questions about whether a particular use is acceptable, the user is expected to speak to a supervisor (for employees) or teacher or administrator (for students and all other users) before engaging in the particular use.

Acceptable Use - District-Issued Technology (Including One-To-One Programs)

The District may issue technology to users, including students and employees, for educational or extra-curricular purposes and/or District business, including through a one-to-one program. Use of District-issued technology is governed by this AUP, including the Acceptable and Unacceptable Use provisions of this AUP, regardless of when, where, or for what purpose the use occurs. This includes use that occurs outside of normal school hours (for students), before or after work times (for employees), for personal purposes, and/or off District property or away from related events or activities.

The user is responsible for reasonable care of District-issued technology at all times during which the technology is issued to the user, regardless of whether the technology is on school property or at related events or activities. This includes the requirement that the user not allow others to use the technology without authorization from an administrator. The procedures implemented by the Superintendent or designee for this AUP may contain further guidelines regarding responsible use, as may handbooks and other guidelines issued at the school level. Costs associated with repair or replacement of technology damaged as a result of a user's failure to exercise reasonable care shall be the responsibility of the user, including any fees for insurance premiums and deductibles, regardless of whether the damage is caused by the user or a third party.[1] Users may be required to obtain and/or pay for insurance for District-issued technology in order to be issued such technology by the District.

Students may only use or access District-issued technology outside of school with parental or guardian approval. The District is not responsible for unacceptable use of District-issued technology by students at any time, including outside of school, although students may face consequences for such misuse under this and other District policies.

Unacceptable Use – General

Users are expected to conform to general expectations of norms outlined in this AUP and other District policies when using the District's electronic resources. This AUP sets forth some general examples of unacceptable use, but does not attempt to set forth all prohibited uses.

The following are examples of uses of the District's electronic resources that are strictly prohibited:

- Any use at a time or in manner that is not authorized or approved, or in a manner that causes or reasonably could be foreseen to cause a substantial and material disruption to the educational environment or invasion of the rights of others;
- Knowingly or recklessly causing a security breach or disruption of service to an individual or system;

- Damaging District electronic resources or the electronic resources of others via District electronic resources, including accessing or attempting to access any content to which the user is not authorized, including "hacking";
- Misrepresenting one's identity or using another person's password, user profile, or technology or allowing another to use one's identity, password, or technology without authorization;
- Any use in a manner that violates State or federal law including using materials that are subject to intellectual property laws, such as copyright and trademark laws, without authorization;
- Any use that violates any Board policy, including policies addressing bullying, harassment, and hazing, and student and employee discipline policies or codes of conduct;
- Publishing or transmitting private information, including photographic, video, and audio depictions of others, without authorization;
- Any transmission, access, creation, or transmission of material that is sexually graphic or explicit, obscene, threatening, intimidating, abusive, harassing, or otherwise indecent, or that reasonably could be interpreted as promoting illegal activity, including illegal drug use;
- Any use for a commercial purpose where the user does not have the express written authorization of the Superintendent or designee;
- Uploading or downloading material, including software, without express authorization of a member of the District's technology staff;
- Accessing or participating in any games without the express authorization of a supervisor (for employees) or teacher or administrator (for students and other users), or using the District's electronic resources for more than incidental[2] personal use;
- Providing personal information, including photographs, about themselves or another; and
- Any attempt to do any of the above.

A user should notify the District's Complaint Manager or Nondiscrimination Coordinator immediately upon receipt of a communication through the District's electronic resources that the user believes is inappropriate or that makes the user feel threatened or uncomfortable.

Internet Filtering, Safety, and Security Measures

The District will implement technology protection measures on each District computer with Internet access, including filtering devices to block user access to visual depictions of material that is obscene, pornographic, or otherwise harmful to minors as defined by the Children's Internet Protection Act (CIPA). The procedures implemented by the Superintendent or designee for this AUP shall allow users to make requests, including anonymous requests, to disable the filter for bona fide research or other lawful purposes.

The District also will take steps, to the extent practical, to promote the safety and security of users of its electronic resources. The steps taken shall include efforts to prevent inappropriate network use such as: (a) unauthorized access, including "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors. The steps taken also shall include efforts to protect student and employee privacy, safety, and security when using electronic communications.

The District and its employees shall take steps, to the extent practical, to educate, supervise, and monitor students' uses of electronic resources as required by CIPA and other federal and state laws.

Confidentiality of Private Information

Users of the District's electronic resources must comply with all policies and procedures that govern confidentiality of private information, including policies governing school student records and personnel records or information, when using the District's electronic resources.

Maintenance of Records

Certain laws require the District to maintain business records, including public records, school student records, and personnel records, for certain periods of time. Users of the District's electronic resources are responsible for maintaining records as required by District policy, District procedures, and/or relevant laws. This may include maintaining school student records and local records as required by state and federal law.

Disclaimer, Limitation of Liability, and Indemnification

The District does not guarantee the quality of the services provided through its electronic resources. The District makes no guarantees about the accuracy of information accessed through its electronic resources. The District is not responsible for: (i) any loss or damages resulting from the unavailability or failure of its electronic resources; (ii) any information that is rendered unavailable because of its electronic resources or lack thereof; or (iii) any inaccurate information accessed through its electronic resources.

All users assume full responsibility for any costs, liabilities, or damages arising from their use of the District's electronic resources, and must reimburse the District for any loss, including reasonable attorney's fees, incurred as a result of their use to the extent allowed by law. The District is not liable for the actions of users of its electronic resources.

No Expectation of Privacy

Users of the District's electronic resources have no expectation of privacy with respect to use of the District's electronic resources, including access of the District's Internet or Wi-Fi using personal technology, or with respect to any material created, transmitted, accessed, or stored via District electronic resources. This includes material created, transmitted, accessed, or stored for personal use, including incidental personal use, on or through the District's electronic resources. The District reserves the right to monitor users' activities on District electronic resources at any time for any reason without prior notification; to access, review, copy, store, and/or delete any electronic information accessed or stored therein; and to disclose such information to others as it deems necessary and/or as required by law. Users should be aware that information may remain on the District's electronic resources even after it has been deleted by the user. This section of this policy may only be altered through amendment of this policy, and may not be altered or diminished by the verbal or written assurances of any employee or representative of the District.[3]

Section II: Student Use of Personal Technology for Educational Purposes (Student BYOD or BYOT)

Applicability

This section applies to all students of the District.

Authorized Use of Personal Technology for Educational Purposes

The Superintendent or designee may authorize students to use personal technology for educational and/or extracurricular purposes, including for classroom instruction and extracurricular activities.

A BYOD or BYOT program authorized by the Superintendent or designee may include use of personal social media websites of students. Students must meet qualifications for holding an account from the social media website and must be authorized by a parent/guardian to utilize a particular social media website before using that website for educational purposes.

Students may use BYOD or BYOT technology on District property or at related events and activities only at times, at places, and for purposes expressly permitted by the BYOD or BYOT program or school personnel. When a student uses personal technology at a time, at a place, in a manner, or for a purpose authorized by the BYOD or BYOT program, the student's use of the personal technology is governed by Section I of this AUP, all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources. At all other times while on District property or at related events and activities, students must comply with requirements for the use of personal technology on District property or at related events and activities outlined in Section IV of this AUP, even if the personal technology device used is one that is authorized for use in a BYOD or BYOT program.

Section III: Employee Use of Personal Technology to Conduct District business (Employee BYOD or BYOT)

Applicability

This section applies to all employees of the District.

Authorized Use of Personal Technology to Conduct District Business

District employees are expected to use the District's electronic resources, as that term is defined in this AUP, to conduct District business when such technology is available, and to request to use personal technology only when a District electronic resource is not available. This includes using District email accounts to conduct written District business with members of the District community whenever practicable.

The Superintendent or designee may authorize employees to use personal technology to conduct District business. With respect to communicating with students when conducting District business, the Superintendent or designee only may authorize use of personal technology to communicate with designated groups of students. If the Superintendent or designee elects to allow such communications with groups of students, the Superintendent or designee shall create an administrative procedure which, along with handbooks and guidelines at the building level, shall govern such use.

For the most part, employees of the District have no need to use social media to conduct District business. In certain cases, the District may decide that such use is in the District's interest and may authorize particular employees to use specific social media tools within guidelines established by the District. Absent such authorization, use of social media accounts, including personal social media accounts, is prohibited for conducting District business. Any social media accounts used to conduct District business must be created using the employee's District-issued email account, and the employee must provide a copy of any user name, account passwords, or other information related to the account to building administration when the account is created and any time the account information is changed.[4] Any user names, accounts, passwords, etc. used to conduct District business and any communications or information contained in or transmitted via such an account are the sole property of the District to the full extent permitted by any applicable law, or user or license agreements. This includes "followers," "contacts," and "friends" associated with any account used to conduct District business. Social media tools not provided by the District should not be used to conduct District business, including communicating with members of the District community when conducting District business.

When an employee uses personal technology to conduct District business, the employee's use of the personal technology is governed by Section I of this AUP and all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources. At all other times on District property or at related events and activities, employees must comply with requirements for the use of personal technology on District property or at related events and activities outlined in Section V of this AUP, regardless of whether the personal technology device used is one that is authorized for use to conduct District business.

No Expectation of Privacy

District employees and representatives may not request personal social networking passwords or information from strictly personal social networking websites from current or prospective employees unless authorized by law. Nothing prevents the District from obtaining and relying on publicly available information from employee personal social networking websites.

Moreover, nothing prevents the District from requesting and, in some cases, requiring access to personal technology and/or related account paperwork for personal technology used by the employee to conduct District business, or from reviewing information related to District business stored on such technology or related paperwork. When using personal technology to conduct District business, employees have no expectation of privacy in material that is stored, transmitted, or received via that technology or related paperwork and agree that the District may request and, in some cases, require the employee to relinquish control of that technology and/or related paperwork for the District's legitimate business purposes. Examples of legitimate business purposes include installing necessary software or hardware, responding to information requests, and investigating allegations of misconduct by employees or students.

The District will take reasonable steps to limit access to employee personal technology used to conduct District business and related paperwork to only that access necessary to obtain and review information related to District business. It may, however, be necessary for the District incidentally to view or review personal information contained on personal technology and/or related paperwork in order to access information related to District business.

This section of this policy may only be altered through amendment of this policy, and may not be altered or diminished by the verbal or written assurances of any employee or representative of the District.

Section IV: Student Personal Use of Technology

Applicability

This section applies to all students of the District when on District property and at school related events and activities.

Acceptable and Unacceptable Personal Use of Technology on District Property and at Related Events and Activities

Students may bring personal technology on District property and to school related events and activities, but must keep such technology in silent mode at all times except when using the technology in an approved BYOD or BYOT program or during an emergency.

Student use of technology, including District electronic resources and personal technology, on District property and at school related events and activities must comply with Section I of this AUP, all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources.

Section V: Employee Personal Use of Technology

Applicability

This section applies to all employees of the District when on District property and at school related events and activities.

Acceptable and Unacceptable Personal Use of Technology on District Property and at Related Events and Activities

District employees may bring personal technology on District property and to school related events and activities and may keep such technology powered on but must keep such technology in silent mode at all times during the work day.

Personal Communications with Members of the District Community

Employees are prohibited from using technology to communicate with a student for personal purposes if they do not have a legitimate independent relationship with the student. Examples of a legitimate independent relationship include a familial relationship or pre-existing relationship through an outside organization such as a religious house of worship. This prohibition includes communicating with students through electronic mail, personal messaging programs or text messaging, and "friending" or "following" students' social media profiles for personal purposes. If an employee has any doubt about whether a legitimate independent relationship justifies an exception to this prohibition, the employee is expected to speak with the Superintendent or Building Principal regarding the relationship prior to deviating from this prohibition.

How an employee otherwise uses technology to communicate with other members of the District community for personal purposes is within his or her own discretion. In general, what employees do on their own time is their affair. However, activities outside of work that may adversely affect an employee's job performance, the performance of others, members of the District community, or the ability of the District to provide efficient services or conduct its business operations may be the subject of discipline. Employees are strongly encouraged to take steps to strictly control the privacy of their online activity, although such measures may not prevent the imposition of discipline.

Disclaimer, Limitation of Liability, and Indemnification

An employee who uses personal technology for personal purposes on District property, at school related events or activities, or with members of the District community, agrees by such use to assume all risks associated with such use, including the risk that students may view or gain access to inappropriate material through the employee's personal technology or that suspicions may arise regarding the nature of a relationship between and employee and a student. Unless the employee is using personal technology to access the District's Internet services, filters may not necessarily be in place to control or monitor use of an employee's technology. It is thus the employee's responsibility to prevent any risks associated with the use of personal technology. An employee will be responsible to indemnify, hold harmless, and defend the District, to the extent allowed by law, for any use of technology for personal purposes, on District property, at school-related events or activities, or with members of the District community that violates this policy, any other District policy, or any relevant law.

Section VI: Internet Publications and District Social Media

Applicability

This section applies to all students and employees of the District who establish and/or operate Internet publications and/or social media websites ("websites") for educational, extra-curricular, or other purposes related to District business, and any other individual operating or attempting to operate a website suggesting approval by or official affiliation with the District.

Official District Websites

Only the Superintendent or designee may operate or approve for operation by District employees official websites on behalf of the District, including the District's website, blogs, and social media accounts. No third-party website may suggest that it is an official District website without the express written authorization from the Superintendent or designee. No website shall be operated using the District's logos or other marks in a manner suggesting approval by or official affiliation with the District without express written authorization from the Superintendent or designee.

Other Websites

Employees and students who wish to establish websites for educational, extra-curricular, or other purposes related to District business, including websites for departments, student courses, field trips, fundraisers, and clubs and teams, must obtain prior written authorization from the Superintendent or designee. Administrative procedures implementing this policy shall set forth the manner by which authorization must be requested and the factors the Superintendent or designee will consider in addressing such requests. No students shall be authorized to establish or operate a website by the District unless an employee of the District agrees to supervise the website.

Monitoring Responsibilities

Employees assigned to operate the District's official websites, employees or students who are authorized to operate websites for educational, extra-curricular, or other purposes related to District business, and employees who supervise students operating authorized websites are responsible for maintaining and monitoring those websites. The administrative procedures implementing this policy shall set forth maintenance requirements, including the requirement that content be kept current and accurate and comply with all relevant laws and District policies and procedures, including Section I of this AUP and all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources. The administrative procedures shall also set forth monitoring requirements, including the requirement that user content be monitored on a regular basis by a District employee for compliance with relevant laws and District policies and procedures, including age-appropriateness of content.

Confidentiality, Privacy, and Non Discrimination

All District official websites and websites operated by students and/or employees for educational, extra-curricular, or other purposes related to District business shall comply with relevant confidentiality and privacy policies and laws, including laws governing educational or student records, and non-discrimination policies and laws. No personally identifying student information shall be posted on such websites if a parent/guardian has a written student release of information refusal form on file, except that photographs of and other content created by students while participating in public extracurricular activities, including sports and theater and musical productions, may be used without parental/guardian permission. Employees operating District official websites and websites operated by students and/or employees for educational, extra-curricular, or other purposes related to District business have no expectation of privacy in materials contained on those websites.

Links to Outside Websites and User Contents

Each website operated on behalf of the District or by students and/or employees for educational, extra-curricular, or other purposes related to District business must state clearly that is it not an open or limited open forum for public use. Contributions from the public on a website, through links, comments, and other types of user content, may vary based on the characteristics of the particular website, but in no case does the District intend to create an open forum or a limited open forum over which no control of user content may be exercised.

Employees assigned to operate the District's official websites, employees or students who are authorized to operate websites for educational, extra-curricular, or other purposes related to District business, and employees who supervise students operating authorized websites shall only link to outside websites and allow comments that conform with the publicly stated purpose of the website. The website shall state that links to outside websites and comments from third parties do not constitute an endorsement by the District of the opinions, products, or services presented on any website linked to or listed on a website that is linked to, or of any comment. The administrative procedures implementing this policy may set forth additional requirements and limitations on links to outside websites and/or comments.

Regardless of the characteristics of the website in question, employees assigned to operate the District's official websites, employees or students who are authorized to operate websites for educational, extra-curricular, or other purposes related to District business, and employees who supervise students operating authorized websites shall delete user comments or other submissions that: (i) include vulgar language; (ii) include personal attacks of any kind; (iiI) reasonably can be interpreted as discrimination or animus on the basis of any protected or other immutable characteristic; (iv) contain spam or links to commercial websites; (v) are clearly off topic; (vi) advocate illegal activity; (vii) constitute marketing of particular services, products, or political organizations; (viii) infringe on copyrights or trademarks; (ix) contain personally identifiable medical information or other privileged or confidential information; (x) may compromise the safety or security of the District or its students, employees, or other members of the District community; (xi) do not conform with the purpose of the particular website in question; or (xii) interfere with, disrupt, or adversely affect the school environment, school operations, or an educational function, including comments or other submissions that may reasonably be considered to: (a) be a threat or an attempted intimidation of an employee; or (b) endanger the health or safety of students, employees, or school property.

Section VII: Consequences of Violating AUP

The activities covered by this policy are privileges, not rights. The District reserves the right to place reasonable limits and prohibitions on such privileges. Failure to comply with this AUP and any implementing administrative procedures, handbooks, or guidelines may lead to the loss of such privileges and may lead to other consequences including discipline, referral for civil and/or criminal prosecution, and any other consequence authorized by law.

The District's ability to impose consequences for violations of this AUP is not limited to conduct that occurs on District property, at school related events and activities, or during school/business hours. For example, student or employee misconduct on technology may lead to consequences under this AUP or other District policies and procedures if the conduct materially and substantially interferes with, disrupts, or adversely affects the school environment, school operations, or an educational function, including conduct that may reasonably be considered to: (a) be a threat or an attempted intimidation of an employee; or (b) endanger the health or safety of students, employees, or school property, regardless of when or where that misconduct occurs.

Section VIII: Notification of Policy and Acknowledgement

Any person who accesses the District's electronic resources, uses personal technology to conduct District business, uses personal technology on District property and at related events, or operates Internet and social media websites for the District or for educational, extra-curricular, or other District business purposes agrees by that conduct to abide by the terms of this AUP and any implementing administrative procedures, handbooks, or guidelines.

The District shall communicate to employees this AUP and any implementing administrative procedures, handbooks, and/or guidelines each year at an in-service training.