Acceptable Use of Technology Policy (AUP)

Board of Education

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: Student Personal Use of Technology:** For all students 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. For all students, defining authorized use of technology for personal purposes on District property and at related events and activities.

- **Section III: Employee Use and Personal Use of Technology:** For all employees 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. 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. 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 IV:** 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 V:** Outlining the consequences of violating of the AUP.

- **Section VI:** Setting forth requirements regarding notification and acknowledgement of the AUP by students, employees, and users of the District's electronic resources.

Acceptable Use of Technology Policy (AUP)

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, 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. The District may discipline a user whose personal technology use or other off-site activity causes, or can reasonably be expected to cause, a substantial disruption of the school environment, without regard to whether that activity or disruption involved District technology.

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 and hours 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.

Acceptable Use of Technology Policy (AUP)

"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, including Student, Discipline, general,7:190 and implementing procedures.

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 of Technology Policy (AUP)

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

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. Users, excluding certified staff, 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 supervision. 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 that are strictly prohibited:

- 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;

Acceptable Use of Technology Policy (AUP)

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

- 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;

- Knowingly using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any United States or State regulations including copyright and trademark laws.

- Use that violates 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;

- Transmission, access, creation, or downloading 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;

- Unauthorized downloading of software, regardless of whether it is copyrighted or devirused.

- 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 personal use;

- Intentionally invading the privacy of others by the unauthorized disclosure or dissemination of information of a personal nature.

- Any attempt to do any of the above.

Acceptable Use of Technology Policy (AUP)

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

A user should notify the District's Complaint Manager or Nondiscrimination Coordinator immediately under Board Policy Uniform Complaint Procedure, 2:260 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.

Acceptable Use of Technology Policy (AUP)

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

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;
(iii) any inaccurate information accessed through its electronic resources.

All users assume full responsibility for any costs, liabilities, or damages arising from their willful or knowing violation of this policy and any related procedures and for any damage resulting from their failure to exercise ordinary care and diligence in protecting the District's electronic resources. Users may be responsible to reimburse the District for loss, including reasonable attorney's fees, incurred as a result of their use to the extent allowed by law.

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. Employees will be informed annually of the no expectation of privacy policy, and the entire AUP policy will be accessible to all users on the district website.

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

Applicability

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

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,

Acceptable Use of Technology Policy (AUP)

through a formal BYOD or BYOT program. Each student must return a BYOD or BYOT agreement, created by the Superintendent or designee, signed by both the student and the student's parent/guardian, before participating in a BYOD or BYOT program.

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, and Student Discipline, general, 7:190**.** 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.

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 powered off 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, as well as Student, Discipline, general, 7:190

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

Students will:

1. Adhere to the rules of copyright and assume that any material that they did not create is copyrighted
2. Assume responsibility for school equipment
3. Understand that E-mail, files, search histories are not guaranteed to be private. The District has access and authorization to view, review, and monitor electronic history in order to maintain the system integrity and to monitor responsible use.
4. Properly use access privileges
5. Avoiding impersonations and anonymity
6. Not allow unauthorized users to have access to personal privileges, passwords, or log in information
7. Protect your confidential information

Acceptable Use of Technology Policy (AUP)

8. Take responsibility for all activity that occurs with personal access information
9. Respect the rights of others and protect the privacy of other users
10. Accept responsibility for all material viewed, downloaded, and/or produced.
11. Use technology to enhance learning, research subjects and learn new concepts
12. Be polite, use appropriate language
13. Follow all District procedures and monitor technology usage. Report any suspicious activity.

Students will not:

1. Access, submit, post, publish, display or create any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, religiously offensive, harassing, illegal or other material inappropriate in the school setting.
2. Violate copyright laws or plagiarize material
3. Gain unauthorized access to resources
4. Use someone else's password or identification
5. Attempt to hack into the District server
6. Download music, games, videos or other media that would require a legal license
7. Play games without expressed consent
8. Harass, intimidate, or threaten anyone
9. Defame or impersonate anyone
10. Use hateful language
11. Cyber stalk
12. Access any social media website
13. Deliberately disrupt the system or destroy data by spreading computer viruses
14. Engage in any illegal activity, such as arranging a drug sale, gamble, purchase alcohol, criminal gang activity or threatening the safety of an individual
15. Post personal information or confidential or private information about anyone, including yourself

Section III: Employee 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 Use of Technology on District Property and at Related Events and Activities

Personal Use of Technology

District employees may bring personal technology on District property and to school related events and activities.

Acceptable Use of Technology Policy (AUP)

A. Employees may only use or access technology, including personal and District-issued technology, for personal purposes before or after work times, during their duty-free lunch time, or in emergencies.

   Any use of technology for personal purposes at school or related events or activities must comply with Section I of this AUP and all other District policies, administrative procedures, handbooks and guidelines governing use of the District's electronic resources, and must not be in a manner that adversely affects or reasonably could be foreseen to 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.

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 shall govern such use.

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.

Section III: Employee Use of Technology

While 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

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 Superintendent or designee may request and in some cases, such as suspicion, report of, or information that has been obtained of unprofessional conduct or a violation of Board Policy may require the employee to relinquish control of the technology.

Acceptable Use of Technology Policy (AUP)

Social Media

Using social media as a way to communicate with students creates a number of serious issues for staff, for the student, and for the District and is strongly discouraged. Such communication is very public and may eventually be viewed in public.

Any content staff members publish, pictures they post, or dialogue they maintain, whether in Facebook, Twitter, a blog, a discussion thread or other website, should never compromise the professionalism, integrity and ethics as a District employee.

In certain cases, the District may decide that the use of social media 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 professional 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. 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 be initially approved through the BYOD or BYOT administrative procedure and includes social media that is used to communicate with members of the District community, including students, when conducting District business.

Section III: Employee Use of Technology

Reimbursement for Use

In some circumstances, employees may be reimbursed for charges associated with the authorized use of personal technology to conduct District business. Reimbursement shall only be allowed if the employee has entered into a written agreement with the District prior to incurring the charges to be reimbursed and if the reimbursement is within budget constraints approved by the Board of Education. If the Superintendent or designee elects to allow such reimbursement, the Superintendent or designee shall create such written agreement and is authorized to create administrative procedures which, along with handbooks and guidelines at the building level, shall set forth the terms for such reimbursement within budget constraints approved by the Board of Education.

No Expectation of Privacy

District employees and representatives may not request personal social networking passwords or information from professional 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.

Acceptable Use of Technology Policy (AUP)

The District has the right to access, search, read, inspect, copy, monitor, log or otherwise use data and information stored, transmitted and processed on the network and computer resources in order to execute the requirements of this policy. Network including but not limited to Internet and E-mail usage may be monitored and audited by the Superintendent and/or designee for inappropriate activity or oversight purposes. The District reserves the right to:

1. Access and make changes to the system connected to the network and computer resources to address security concerns
2. Deny user access to the system to address security concerns
3. Determine what constitutes appropriate use of these resources and to report any illegal activities

The Superintendent or designee may request and in some cases, such as suspicion, report of or information that has been obtained of unprofessional conduct or a violation of Board Policy may require the employee to relinquish control of the technology and have 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.

Examples of legitimate business purposes include installing necessary software or hardware, responding to information requests, and investigating allegations of misconduct by employees or students.

Section III: Employee Use of Technology

Personal Communications with Members of the District Community, Including Students

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. Staff communication with students should be public, transparent, collaborative, secure and professional. Always choose words that are courteous, conscientious and generally business like. Any use of social media must be approved by the Superintendent or designee. Staff are discouraged from communicating with students in any way that could potential be perceived as inappropriate or a personal relationship with sharing of personal and private information.

The District provided methods of communication are the most appropriate and only communication allowed without expressed written permission. For example, Blackboard allows for effective online learning by supporting online discussions, secure chat rooms, online delivery of assessments, and the sharing of documents, images, and other media all in a secure, password protected environment.

Acceptable Use of Technology Policy (AUP)

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 uses technology to communicate with 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.

Section III: Employee Use of Technology

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. The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any intentional or reckless breach of this policy including such incurred through copyright violation.

In the event that a teacher action requires a conference that can reasonably be expected to result in a letter of reprimand or some other form of serious disciplinary actions, the teacher will be informed of the nature of the conference and the right to a representative. If discipline is deemed necessary, the administration will give written notice of the specific grounds forming the basis for the discipline to the employee and, upon request by the employee to the Association.

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 Superintendent or designee 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.

The actions of the users accessing networks reflect on the District; therefore, users must conduct themselves accordingly by exercising good judgment and complying with this policy, and any accompanying administrative regulations and guidelines.

Acceptable Use of Technology Policy (AUP)

Section III: Employee Use of Technology

Staff will:

1. Adhere to the rules of copyright and assume that any software that they did not create is copyrighted
2. Adhere to the licensing agreements governing the use of software
3. Note that e-mail is not guaranteed to be private. People who operate the system do have authorization to mail; others may have access
4. Be responsible at all times for the proper use of their access privileges and for avoiding impersonations, anonymity, or unauthorized sharing of security measures
5. Take responsibility for any activities using technology that is borrowed by them or under their account or password
6. Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses
7. Respect the right of others to use equipment and therefore not use it for non-school activities, with exception of personal incidental use
8. Abide by the policies and procedures of networks and systems linked by technology
9. Protect the privacy of other users and the integrity of the system by avoiding misuse of passwords, others' files, equipment, and programs

Staff will not:

1. Use offensive, obscene, inflammatory or defamatory speech
2. Harass other users
3. Use the account of another user
4. Misrepresent themselves or others
5. Violate the rights of others, including their privacy
6. Access, download, and/or create pornographic or obscene material
7. Use the network for personal business or financial gain
8. Vandalize data, programs, and/or networks
9. Degrade or disrupt systems and/or equipment
10. Damage technology, hardware and/or software
11. Spread computer viruses
12. Gain unauthorized access to resources or entities
13. Violate copyright laws
14. Use technology for illegal activities

Acceptable Use of Technology Policy (AUP)

Section IV: 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

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.

Acceptable Use of Technology Policy (AUP)

Section IV: Internet Publications and District Social Media

Release of Student Names, Photographs or Original Work

The district and its schools will be allowed to use student names, photographs and original work for publicity efforts, unless instructed in writing by a student's parent/guardian not to do so. Student first and last names may be used on District Web sites for middle and high school students. Elementary school student names will not be published online. Publicity efforts may include, but are not limited to: district publications, videos and Web sites; and placements in local, regional and national media (both print and electronic).

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 will 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. Employees will be given examples and/or guidance from administration with what constitutes a clear statement.

Section IV: Internet Publications and District Social Media

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, as defined by the First Amendment;
- **(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 V: 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.

Employees in violation of this policy, administrative procedures, handbooks, or other related AUP policies will be afforded all their contractual and statutory rights if discipline is imposed.

Acceptable Use of Technology Policy (AUP)

Section VI: Notification of Policy and Acknowledgement

All students, employees, and users of the District's electronic resources are required to sign and return to the District an acknowledgement form indicating that the user has reviewed, understands, and agrees to abide by this AUP and any related administrative procedures, handbooks, and guidelines. A parent/guardian of each student must also sign and return an authorization form. Any person who fails to return a signed authorization form as required by this Section shall be refused the privileges of accessing or using the District's electronic resources, using personal technology for educational purposes or District business, using personal technology on District property and at related events, and operating Internet and social media websites for the District or as a student or employee of the District. A signed authorization form shall remain valid and on file indefinitely, although the Superintendent or designee may require a new form be completed from time to time.

Even if there is no signed form on file, 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.

Students shall be provided age-appropriate training regarding the standards and acceptable use of the District's electronic resources; Internet safety; appropriate behaviors while online, on social networking websites, and in chat rooms; cyberbullying awareness and response; and other requirements for compliance with CIPA and other federal and state laws before use of the District's electronic resources or technology for educational purposes begins. The District shall communicate to students regarding this AUP and any implementing administrative procedures, handbooks, and/or guidelines each year through a training or the curriculum.

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

ADOPTED: January 26, 2015