SUBJECT: STAFF ACCEPTABLE USE

The District's computer system (DCS hereafter) is provided for staff to enhance the educational programs of the District, to further District goals and objectives; and to conduct research and communicate with others.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance apply to use of the DCS. The standards of acceptable use as well as prohibited conduct by staff accessing the DCS, as outlined in District policy and regulation, are not intended to be all-inclusive. Any staff member who commits an act of misconduct that is not specifically addressed in District policy and/or regulation may also be subject to disciplinary action, including loss of access to the DCS as well as the imposition of discipline under the law and/or the applicable collective bargaining agreement. Legal action may also be initiated against a staff member who willfully, maliciously, or unlawfully damages or destroys property of the District.

Staff utilize electronic communications in their roles as employees of the District. Staff are also encouraged to utilize electronic means to exchange communications with parents or guardians or homebound students, subject to appropriate consideration for student privacy. This usage will be limited to school related issues or activities. Communications over the DCS are often public in nature; therefore, general rules and standards for professional behavior and communications apply.

Privacy Rights

Staff data files, email, and electronic storage areas remain District property, subject to District control and inspection. The computer coordinator may access all files and communications without prior notice to ensure system integrity and that users are complying with requirements of District policy and accompanying regulations. Staff should not expect that information stored on the DCS will be private.

Prohibitions

In addition to the general requirements of acceptable staff behavior, activities which are prohibited by staff members include, but are not limited to, the following:

1) Using the DCS which in any way results in unauthorized charges or expense to the District.

2) Damaging, disabling, or otherwise interfering with the operation of computers, computer systems, software, or related equipment through physical action or by electronic means.

3) Using unauthorized software on the DCS. All software, programs, and applications on the DCS and/or District-owned devices must be approved by, downloaded, and/or installed by the District's Information Technology Department or his or her designee.

4) Changing, copying, renaming, deleting, reading, or otherwise accessing files or software not created by the staff member without express permission from the computer coordinator.

5) Violating copyright law, including the illegal file sharing of music, videos, and software.

6) Employing the DCS for commercial purposes, product advertisement, or political lobbying.

7) Disclosing an individual password to others or using others' passwords.

8) Sharing confidential information on students and employees. Administrative or staff access is limited to portions of the DCS necessary for the staff member to perform his or her job responsibilities. Access to unauthorized areas of the DCS is prohibited due to the confidential nature of the information contained therein.

9) Sending or displaying offensive messages or pictures.

10) Using obscene language.

11) Harassing, insulting, bullying, threatening, or attacking others.

12) Engaging in practices that threaten the DCS (e.g., loading files that may introduce a virus).

13) Violating regulations prescribed by the network provider.

14) Use of the DCS for other than school related work or activities.

15) Assisting a student to violate District policy and/or regulation, or failing to report knowledge of any student violations of the District's policy and regulation on student use of computerized information resources.

16) Use which violates any other aspect of District policy and/or regulations, as well as local, state, or federal laws or regulations.

Any user of the DCS that accesses another network or other computer resources shall be subject to that network's acceptable use policy.

Sanctions

The Information Technology Department computer coordinator will report inappropriate behavior to the staff member's supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations, or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the DCS and/or disciplinary action. When applicable, law enforcement agencies may be involved.

(Continued)

Notification

All staff will be given a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Each staff member will sign an Agreement for Staff Acceptable Use (Form #6410F) before establishing an account or continuing their use of the DC

SUBJECT: SOCIAL MEDIA GUIDELINES FOR EMPLOYEES

Social media and social networking sites (SNS) have great potential to connect people around the globe and enhance communication; however, they are also informal, less structured, and subject to constant change. These guidelines establish some basic parameters on the creation and use of SNS and other social media for the District and its personnel.

"Public social media networks or Social Networking sites (SNS)" are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other social media generally available to the public or consumers and which do not fall within the District's electronic technology network (e.g., Facebook, Instagram, Twitter, LinkedIn, Snapchat, TikTok, blog sites, etc.). "District approved password-protected social media tools" are those that fall within the District's electronic technology network or which the District has approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access within these internal forums.

Official District Use

"Official District use" is defined as the use of social media by an employee, on behalf of his or her department, program or school that has been authorized for the express purpose of communicating the District's broad interests or specific programmatic and policy interests. The authorization may be granted by the Superintendent or designee. There are also many official uses of social media that are not public, such as the use of internal blogs or wikis for collaboration among grade-level or project teams. Employees are prohibited from setting up public SNS for any official District use related to their division, building, or service unless they have obtained prior approval in accordance with the procedures set forth below.

Establishing a Social Networking Site for Official District Use

1) Following approval from the appropriate building principal and/or public relations designee or Technology Coordinator, the public relations or technology staff will work with the department, building, or service to properly set up an appropriate SNS. All account names and log in passwords must be on file in the Technology Department.

2) The Superintendent or designee will have the exclusive and final authority to determine whether individual buildings or facilities may initiate and maintain separate page(s) on the SNS.

Quality Control/Content Integrity

1) The District will provide general training for all applicable personnel, including training on ethical and legal considerations, and compliance with all applicable policies and regulations.

2) The official District website will remain the primary source for all content.

SUBJECT: SOCIAL MEDIA GUIDELINES FOR EMPLOYEES (Cont'd.)

3) Do not post confidential or proprietary information about the District, its students, alumni, or employees. Use good judgment and follow District policies and laws or regulations related to student privacy.

4) Thoroughly check your content for spelling and grammar before posting.

Disclaimers

As a public entity, the District will include disclaimers on their site regarding grounds for removal of comments and the frequency to which the site is monitored.

Professional or Classroom Use

"Professional use" is defined as an employee's use of social media for the purpose of furthering his or her specific job responsibilities or professional duties through an externally focused site or a District sponsored site. While use for professional interests is beneficial to the work of the District because it enables employee to stay informed on important issues or to collaborate with their peers, the social media tool or site the employee is using is not maintained or monitored by the District itself. Employees' participation in external social media for professional use, using district technology, equipment, and email addresses or during the school day requires prior approval and is subject to the procedures set forth below.

"Classroom use" is defined as use of SNS in a classroom for instructional purposes. Students can interact with their peers and their teacher to discuss a current class topic, sharing what they have discovered on the internet and voicing their opinions. Teachers can upload homework, post school notices, moderate discussions, and share materials. This online portal develops writing skills, encourages research skills, and promotes intellectual discussion. Staff must also obtain prior approval for classroom use of these internal forums.

Establishing Access

1) If you are participating in a SNS and/or blog for District-related professional use, it must be done with the approval of your supervisor or principal.

(Continued)

SUBJECT: SOCIAL MEDIA GUIDELINES FOR EMPLOYEES (Cont'd.)

2) Use of outside SNS (such as Facebook) for classroom or instructional purposes is discouraged**.*** The District does not permit any communication or contact between staff and students on non-district based SNS (i.e., Facebook, Twitter, etc.). Teachers are encouraged to use existing District or RIC established web tools such as teacher web pages within the District website to communicate with students, to assign and collect student work, or to provide online feedback to students.

3) The District may establish an Alumni page within its District SNS. Teachers and staff may interact with former students within this forum on the district site. Staff interaction with former students outside of the district controlled environment is prohibited. Use caution when "friending" former students. Realize that many former students have online connections with current students. Information shared between school staff and former students is likely to be seen by current students as well.

4) If you would like to request that a "blocked" online site be accessible to use for teaching and learning, submit a request to the Information Technology Department. Requests will be reviewed and the District list of blocked sites will be updated throughout the school year. A description should be provided of the intended use of the site and what tools on the site match your needed criteria. A link to the privacy policy for these sites should also be included.

Quality Control/Content Integrity

1) When using social media for professional purposes, always identify yourself and your position with the District. Use your actual name - never create an alias or post as anonymous. Misidentifying yourself or providing false information may result in disciplinary action. The District email address attached to your name implies that you are acting on behalf of the District.

2) District personnel acknowledge and agree that when they create or post material on the District SNS they are in effect "content publishers" and as such, are subject to a host of ethical and legal obligations including, but not limited to, compliance with the federal Digital Millennium Copyright Act.

(Continued)

SUBJECT: SOCIAL MEDIA GUIDELINES FOR EMPLOYEES (Cont'd.)

Personal Use and Responsibility

"Personal use" is defined as use that is not related to an employee's job duties for the District or his or her professional interests. An employee checking his or her personal Facebook page, sending out a personal Tweet, or watching the latest viral YouTube video are examples of personal use of social media during the work day.

1) The District does not allow personal use of social media during work hours and on District owned hardware. *However, limited personal use of social media during the work day may be permitted on non-district owned personal computers or devices.

2) District employees are personally responsible for all comments and information they publish online.

3) Social media sites require an email address to register and begin use. District employees should not use their work email address for registering or logging in to any SNS.

4) Online behavior should reflect the same standards of honesty, respect, and consideration that are used in face-to-face contact, and be in accordance with the highest professional standards. Online activities or communications which are improper, unethical, illegal, or which cause undue discomfort for students, employees, parents, or other members of the school community should be avoided.

5) Posting comments and having online conversations on social media sites makes those comments public and available to anyone who has any online access. Please be aware that even with the strictest privacy settings what is said online should be within the bounds of professional discretion.

6) Comments related to the District should always meet the highest standards of professional discretion. When posting, employees should act on the assumption that all postings are in the public domain. Remember that posted information could be interpreted as an extension of your office or classroom. What is inappropriate in your office or classroom is also inappropriate online. If posting comments or viewpoints on topics related to the District using any online medium be sure you state that the information is representative of your views and opinions and not necessarily the views and opinions of the District.

7) Before posting personal photographs or avatars that represent you, consider how the images reflect on your reputation and professionalism. Also, remember not to use copyrighted images.

8) District personnel should not use personal SNS to create or maintain personal relationships with students. For purposes of these guidelines, "personal relationships with students" means any behavior or conduct that is unrelated to course work or official school matters.

(Continued)

SUBJECT: SOCIAL MEDIA GUIDELINES FOR EMPLOYEES (Cont'd.)

If an employee position within the District calls for communication with students or parents and is educationally justifiable, the use of the District network, email, teacher web pages within the District website, and school-provided or owned equipment are suggested for use when communicating on-line.

9) While mindful of employees' First Amendment free speech rights, District personnel who participate in social networking websites, including the District SNS, will not post any material which may result in the disruption of classroom or District activities. The District is entitled to make this determination based on the facts surrounding the material as the District reasonably believes them to be.

Employees are encouraged to seek permission from the subject before posting photographs and videos of fellow employees taken on school property or at school sponsored events. Due to the sensitive nature and potentially damaging consequences, posting photographs or information about currently enrolled students in any capacity is prohibited.

School Logos

Within your personal social mediums, do not use any District or school logo without written permission from District officials. For official pages, the District will provide you with a profile image to use.

Reporting Requirements

District personnel will be required to report known or suspected violations of the District SNS Guidelines to their building principal or immediate supervisor.

Disciplinary Sanctions

District personnel who violate any provision of the SNS guidelines will be subject to appropriate disciplinary measures up to and including termination of employment in accordance with legal guidelines, District policy and regulations, and any applicable collective bargaining agreement.

SUBJECT: STAFF USE OF PERSONAL TECHNOLOGY

All staff who use mobile technology in the course of their job duties, including but not limited to cell phones, smart phones, flash drives, tablets, e-readers, laptop computers, scanners, printers, digital cameras, camcorders, PDAs, iPads and iPods, must comply with this Regulation which governs the use of this type of equipment. Any device that runs software or systems including, but not limited to, Palm OS, Windows, Pocket PC, Android or IOS is considered a "computer" for the purposes of this Regulation. In addition, all applicable language in Policy #6410 and Regulation #6410R -- Staff Acceptable Use and Form #6410F -- Agreement for Staff Acceptable Use also applies to all personal technology equipment when it is used in conjunction with the District's wireless network or in the course of the staff member's job duties.

Access to confidential data is a privilege afforded to District staff in the performance of their duties. Safeguarding this data is a District responsibility that the Board takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use personal devices to access the District Computer System (hereinafter "DCS") and the information contained therein.

Confidentiality and Private Information and Privacy Rights

Confidential and/or private data, including, but not limited to, protected student records, employee personal identifying information, and District assessment data, will only be loaded, stored, or transferred to District-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the DCS, any mobile devices, including flash or key drives, and any devices that access the DCS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location and will not use cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

Staff will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after 60 minutes.

Staff data files and electronic storage areas will remain District property, subject to District control and inspection. The Technology Coordinator may access all files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should not expect that information stored on the DCS will be private.

Personally Owned Devices

Staff may choose to use their own personal devices to perform job-related functions, rather than the technology assigned to them by the District. If a staff member chooses to use his or her own personal technology equipment, the following guidelines will apply:

(Continued)

SUBJECT: STAFF USE OF PERSONAL TECHNOLOGY (Cont'd.)

1) Personal devices connected to the DCS or wireless network must have updated and secure operating systems, and have their use segregated from District network resources. Staff must notify Technology staff of their planned use of such a device so proper safeguards can be instituted.

2) The entire cost to acquire all personal technology equipment is the responsibility of the staff member. Services that may incur a financial cost to the District, such as phone options or other "apps" are not allowed.

3) Personal technology equipment is not covered by the District's insurance if it is lost, stolen or damaged. Loss or damage to any personal technology equipment is solely the responsibility of the staff member. If lost or stolen, the loss should be reported immediately to Technology staff so appropriate action can be taken to minimize any possible risk to the DCS and the District.

4) Staff assumes complete responsibility for the maintenance of personal devices, including maintenance to conform to District standards. Staff also assumes all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by Technology staff.

5) Staff must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work purposes (i.e., do not change the format of a file so that the original file is unusable on District-owned hardware or software).

6) All personal technology equipment used on the DCS or wireless network is subject to review by the District Technology Coordinator, or individuals or entities designated by the Superintendent, if there is reason to suspect that the personal device is causing a problem to the DCS network, or if the staff member is suspected by a supervisor of spending excessive time at work on non-work related matters.

7) The District's email client will not be installed on personally owned devices. All access to email and personnel forms will be through employee access on the District webpage, or by accessing the Traveler module from the wireless network or the personal data plan of the user's device.

(Continued)

8) The use of personal technology equipment in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). The staff is required to submit any such information or equipment, when requested.

9) It is also the responsibility of District staff using a mobile device, personal or District-owned, to ensure that all security protocols normally used in the management of District data on conventional storage infrastructure are also applied on that mobile device. All District-defined processes for storing, accessing, and backing up data must be used on any device used to access the DCS.

10) Staff may access the DCS remotely if the staff member has demonstrated that his or her personal device meets the security standards set by the District.

11) Use of any mobile technology device during the school day, whether District-issued or personally owned, should not interfere with the staff member's ability to carry out daily responsibilities.

Flash Drives

Flash or key drives may be provided to staff members for use on the District network if required by their job responsibilities. Flash drives that contain private and personal secure information (PPSI) will be encrypted and/or password protected. Flash drives that contain material such as PowerPoint presentations or general District or budget information do not need to be encrypted. Use of a personally owned flash drive to conduct District business is prohibited.

Wireless Devices on District Premises

1) For security reasons, staff who use their personal device to connect to the Internet, using a District network, will only be permitted to use the District's wireless network. Access to any other District network using a personal device is prohibited.

2) Personal devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any District building. Any staff member who violates the conditions of this regulation using his or her own device will have his or her access privileges withdrawn.

3) When personal devices are used in District facilities or on the District wireless network, the District reserves the right to:

(Continued)

SUBJECT: STAFF USE OF PERSONAL TECHNOLOGY (Cont'd.)

a. Make determinations on whether specific uses of the personally owned wireless devices are consistent with the Staff Acceptable Use of Technology agreement;

b. Log network use and monitor storage disk space utilized by such users; and

c. Remove or restrict the user's access to the network and suspend the right to use the personally owned computer in District facilities at any time if it is determined that the user is engaged in unauthorized activity, violating the District's Staff Acceptable Use of Technology agreement, or violating the terms of this Regulation.

BASE SCHOOL DISTRICT
AGREEMENT FOR STAFF ACCEPTABLE USE

In consideration for the use of the District's Computer System (DCS), I acknowledge that I have been provided with a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. I agree to adhere to the staff policy and the regulations and to any changes or additions later adopted by the District. I also agree to adhere to related policies published in the Staff Handbook. I will report all violations of the District's policy on use of computerized information resources to District officials.

All technology tools provided to staff are the property of the District and fall under the guidelines listed below. This Agreement applies to all District technology resources including, but not limited to, on- and off-site use of blogging, social networking sites and tools, wikis, and podcasting or broadcasting tools provided by the District. In addition, employees who use personal technology equipment to perform job duties, including, but not limited to, cell phones, computers, tablets, smart phones, and iPods which are not owned by the District, must comply with this agreement when using their own technology equipment while connected to the District wireless guest network (see Regulation #6410R.2 -- Staff Use of Personal Technology).

Expectations for employee conduct while using these resources include, but are not limited to, the following:

1) Student Personal Safety

   a. Employees who supervise students with access to technology resources will be familiar with the District Regulation #7315R -- Student AUP Guidelines as well as the District *Code of Conduct*, and enforce the provisions outlined in both documents.

   b. Student use of technology will be supervised to the extent appropriate. Digital ethics is the responsibility of all who monitor student use.

2) Illegal or Destructive Activities

   a. Employees will not go beyond their authorized access to the District network or other computer equipment or software. This will include accessing the files or accounts of others without authorization.

   b. Employees will not disrupt or attempt to damage or disrupt any technology tools, infrastructure, network capacity, system performance, or data.

   c. Employees will not use District equipment or personal equipment connected to the District guest network to engage in illegal acts.

3) System Security

   a. Employees are responsible for the security of all technology tools, files, and passwords.

   b. Employees will promptly notify their immediate supervisor of security problems.

   c. Employees with access to student records may not use, release, or share these records (or information contained in these records) except as authorized by federal and state law.

BASE SCHOOL DISTRICT
AGREEMENT FOR STAFF ACCEPTABLE USE (Cont'd.)

d. Employees whose position and responsibilities require a cell phone or other mobile device for District business purposes and who receive that service through the District service plan must notify the District *immediately* if their device is lost or stolen. Employees should contact their immediate Supervisor and/or Technology Coordinator. For District supplied devices, cell and data service will be terminated immediately to protect the organization from unauthorized use.

e. Personally owned flash drives will not be used for District official business purposes.

4) Inappropriate Conduct

a. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language;

b. Potentially damaging, dangerous, or disruptive material;

c. Racial, sexual or other harassment, or bullying in violation of District policies or regulations; and

d. False or defamatory statements.

5) Inappropriate Access to Material

a. Technology resources will not be used to access or disseminate material that is profane, obscene (pornographic), or advocates illegal acts, violence, or illegal discrimination. Inadvertent inappropriate access will be reported immediately to the supervisor.

b. Business use of instant messaging within the email program is allowed for District staff. The use of Internet games, web chats, unauthorized software, or non-authorized instant messaging software (e.g., AOL Instant Messenger, etc.) is prohibited.

c. Use of publicly available non-District created Web collaboration tools such as blogs, wikis, and social networking tools for work purposes is acceptable, if conducted in accordance with Regulation #6410R.1 -- Social Media Guidelines for Employees. Staff must use District authorized resources to create teacher or classroom web pages. Unofficial personal use of social networking sites during the work day and using District technology resources is not permitted without prior supervisor approval initiated by an employee's supervisor. Excessive use of personal technology devices for non-work related activity during the work day is not permitted and may result in disciplinary action.

6) Expectation of Privacy

Employees have no expectation of privacy in files, disks, or documents that have been created in, entered in, stored in, downloaded from, or used on District equipment.

(Continued)

BASE SCHOOL DISTRICT
AGREEMENT FOR STAFF ACCEPTABLE USE (Cont'd.)

7) <u>Discipline</u>

a. Staff members who engage in unacceptable use may lose access to technology tools provided by the District and may be subject to further discipline in accordance with applicable law and collective bargaining agreements.

b. Deliberate violations of this agreement are cause for disciplinary action up to and including termination.

8) <u>Unacceptable Uses</u>

a. Illegal or malicious use, including downloading or transmitting of copyrighted material such as music, videos, and games.

b. To solicit personal information with the intent of using that information to cause emotional or physical harm.

c. To disrupt the work of other users. This includes the propagation of computer viruses and use of the Internet to make unauthorized entry to any other Internet resource.

d. Use for private business purposes. This includes, but is not limited to, the installation or loading of personal business programs onto your computer for your use for tasks not associated with your District job duties.

e. Downloading of music, games, or other programs for personal use, or streaming of music or video for personal use, are prohibited under all circumstances.

I understand that failure to comply with these policies and accompanying regulations may result in the loss of my access to the DCS and may, in addition, result in the imposition of discipline under the law or the applicable collective bargaining agreement. I further understand that the District reserves the right to pursue legal action against me if I willfully, maliciously, or unlawfully damage or destroy property of the District.

Staff Member Signature: ____

Date: _____________

School Building: __________________________________