USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

General System User Responsibilities

Online conduct

- The individual in whose name a system account is issued is responsible at all times for its proper use. The district's system will be used only for educational purposes consistent with the district's mission and goals. The district prohibits commercial and/or personal use of the district's system.

- System users will not submit, publish, or display on the district's system any inaccurate and/or objectionable material.

- System users will not encourage the use of tobacco, alcohol, or controlled substances or otherwise promote any other activity prohibited by district policy or state or federal law.

- Transmission of material, information, or software in violation of any district policy or local, state, or federal law is prohibited.

- System users identifying a security problem on the district's system must notify the appropriate teacher, principal, or district coordinator.

- System users may not use another individual's system account without written permission from the principal or district coordinator as appropriate.

- Attempts by a student to log on to the district's system as a district administrator will result in cancellation of user privileges and may result in disciplinary action up to and including expulsion.

- System users will not write to directories other than their own as identified by the district.

- Any system user identified as a security risk or having a history of violations of district and/or building computer-use guidelines may be denied access to the district's system.

- Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users is prohibited as is deliberate interference with the ability of other system users to send/receive electronic mail.

- System users will not evade, change, or exceed resource quotas or disk usage quotas as set by the principal. A user who remains in non-compliance of disk space quotas after seven (7) calendar days of notification may have his/her file removed by the principal. Such quotas may be exceeded only by requesting to the principal that disk quotas be increased and stating the need for the increase.

- System users will do a virus check on downloaded files to avoid spreading computer viruses. Deliberate attempts to degrade or disrupt system performance will be viewed as violation of district policy and administrative regulations and may be viewed as criminal activity under applicable state and federal laws.

(see next page)

- Vandalism will result in cancellation of system use privileges. Fines will be imposed for acts of vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's system, or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creating of computer viruses.

- Any software having the purpose of damaging the district's system or another user's system is prohibited.

- Copyrighted material may not be placed on any system connected to the district's system without the author's permission. Only the owner or individuals the owner specifically authorizes may upload copyrighted material to the system.

- System users may download copyrighted material for their own use. System users may redistribute non-commercial copyrighted programs only with the express permission of the owner or authorized person. Such permission must be specified in the document or must be obtained directly from the author in accordance with applicable copyright laws, district policy, and administrative rules.

- System users may upload public domain programs to the system. System users may also download public domain programs for their own use or non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

Telephone/Membership/Other changes

- The district assumes no responsibility or liability for any membership or phone charges including, but not limited to, long distance charges, per minute (unit) surcharges, and/or equipment or line costs incurred by any home usage of the district's system.

- Any disputes or problems regarding phone services for home users of the district's system are strictly between the system user and his/her local phone company and/or long distance service provider.

- Commercial and/or personal use of the district's system is prohibited.

Updating member account information

- The district may require new registration and account information from system users to continue service.

- System users must notify the district of any changes of account information such as address and phone number.

- Student account information will be maintained in accordance with applicable education records law and district policy and administrative rules.

Information content/third party supplied information

- System users and the parents/legal guardians of system users are advised that use of the district's system may provide access to other electronic communications systems that may contain inaccurate and/or objectionable material.

 (see next page)

- The district does not condone the use of objectionable materials. Such materials are prohibited in the school environment.

- The parents/legal guardians of students with accounts on the district's system should be aware of the existence of such materials and monitor their student's home usage of the district's system accordingly.

- Students knowingly bringing prohibited materials into the school environment will be subject to suspension and/or revocation of their privileges on the district's system and will be subject to discipline in accordance with the district's policy and applicable administrative rules.

- Staff knowingly bringing prohibited materials into the school will be subject to disciplinary action in accordance with district policy for discipline and dismissal.

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

System access

- The following individuals are authorized to use the district's system:

  - All district employees.

  - Students in grades PK-12. Students will have secure and private individual network accounts similar to those used by staff members.

  - Non-school persons who request guest accounts. Guest account requests may be made to the principal. Requests may be granted on a case-by-case basis consistent with the district's mission and goals and as needs and resources permit.

- Anyone granted a network account is ultimately responsible for the use of the account and is required to maintain password confidentiality.

- Students completing required course work on the system have first priority to district equipment after school hours.

Acceptable Use of Technology

Email usage guidelines

- Prohibit advertising or solicitation of business.

- Prohibit the sending of chain letters.

- Prohibit fundraising.

- Adhere to all rules of email etiquette.

- Adhere to the rules that all emails reflect the views of the school district as each email carries the district's net address.

 (see next page)

- Prohibit transmission of any material in violation of any federal or state laws or regulations to include, but not be limited to, copyrighted material, material protected by trade secret, sexual harassment, or other forms of discrimination.

- Prohibit student and employee access to personal third-party email accounts.

- Require student notification of school personnel upon receipt of any inappropriate emails.

- Prohibit altering any network files or jamming the network with spam mail, viruses, etc.

Internet usage guidelines

- Annually, each school will provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbulling awareness and response.

- Prohibit transmission of any material in violation of any federal or state laws or regulations to include, but not be limited to, copyrighted material, threatening or obscene material, material protected by trade secret, sexual harassment, or other forms of discrimination.

- Require all users to accept the responsibility to safeguard their passwords.

- Prohibit the downloading of software, files, etc., without permission of the network administrator.

- Prohibit access/modification to any files to which the user has not been given appropriate authorization.

- Prohibit the posting of photos of students without administration approval and parental permission.

- Allow the downloading of only material that is not a copyright violation. Copyrighted photos and cartoons are not downloadable, and movie segments are allowable if they are on the ALA approved list.

- Prohibit student participation in any form of electronic “chat” unless it is for specific educational purposes and directly supervised by staff.

- Require staff supervision when students access the Internet.

- Require “safe” and “valid” Internet searching.

- Provide Internet filtering software to decrease the ability of users to access web sites displaying obscene material.

- Prohibit the use of any district technology for the purpose of cyberbullying.

- Prohibit the use of social networking sites except those explicitly allowed by the district.

Network usage guidelines

- Require that repair charges will be assessed to anyone who intentionally damages the network.

- Adhere to all licensing guidelines when loading software.

 (see next page)

- Limit the amount of data that can be stored on the network.
- Adhere to all copyright laws when scanning.
- Install and/or use only that software and hardware approved and/or provided by the district.
- Prohibit altering any network files or jamming the network such as with, but not limited to, spam mail, chain letters, viruses, etc.
- Employees and students are allowed to bring personal computing devices onto district campuses and attach to the "guest" Wi-Fi network. The guest wireless network provides a separate space apart from our secured network allowing devices other than those provided by the district an avenue for accessing the Internet. However, this access is still filtered and monitored to adhere to federal CIPA guidelines and does not provide unrestricted Internet access.
- Use of the guest network follows this same acceptable use policy as it is still district property and offered as a convenience and not a right.
- In the previous three bullets, personal computing devices can be synonymous with laptops, iPads, iPods, iPhones, Android phones, other smart phones, and any other device capable of connecting to the internet via a Wi-Fi connection.
- The district bears no responsibility for any damage, viruses, spyware, etc. that occurs to a personal computing device while on district campuses.
- Abuse or misuse of the guest network can cause the network administrator to block any device at any time from utilization. Examples would include introducing viruses, downloading too much data, connecting to inappropriate sites or inappropriate activity.

Webpage usage guidelines

- Adhere to "public performance" copyright laws, not just "fair use" laws which apply to a classroom only.
- Adhere to all copyright regulations as stated in purchased software such as clip art.
- Assume that materials are copyrighted unless there is a clear statement that art, photos, and/or text are "public domain."
- Publish only information about the school; courses, activities, instructional resources, student handbook, events calendar, principal's message, district mission, menus, meeting dates, testing dates, links to education sites, etc., district and/or school board agendas.
- Adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA) giving public notice that a school may publish "directory information" whereas "education record" information cannot be published. Avoid the publication of a student's photo without parental permission and administration approval.
- Identify a student's intellectual property as first name plus initial of surname.
- As a professional publication, assure grammatical correctness.
- Avoid objectionable material or links to objectionable material.

 (see next page)

- Publish student work only upon receiving parental permission.
- Avoid any links to "page under construction" or other indications of unfinished work.
- Include district email addresses of staff members only; not student email addresses.
- Include the date of update.
- Include the initials of the page creator.
- Refrain from using any student surnames.
- Adhere to all ethical behaviors of the district.
- Include a disclaimer statement.
- Prohibit transmission of any material in violation of any federal or state laws or regulations to include, but not be limited to, copyrighted material, threatening or obscene material, material protected by trade secret, sexual harassment, or other forms of discrimination.
- Prohibit advertising or solicitation of business.

Teacher requirements for class webpages

Webpage requirements

- Every teacher will maintain a class webpage on the district communication platform.
- All posted information must be accurate and up-to-date.
- See the District Technology Plan for more details and specific information.

Hardware usage guidelines

- Prohibit vandalism and/or theft; vandalism includes, but is not limited to, malicious damage to hardware, harm or destruction of software, and/or alteration of another user's data.
- Accept repair assessment charges for the damage or intentional misuse of any equipment to include, but not be limited to, computers, scanners, LCD projectors, digital cameras, etc.
- Prohibit vandalism to include, but not be limited to, removal of the mouse ball and/or mouse, **deliberate** erasing of files and/or data, placing foreign objects (i.e., paperclips) in disk/CD drives, removing or altering keyboard keys, etc.
- Prohibit the use of video cameras or digital cameras for any use other than to support the mission of the district.

Internet acceptable use/safety

Student Internet activities will be monitored by the district to ensure students are not accessing inappropriate sites that have visual depictions that include obscenity or child pornography or are harmful to minors. The school district will use technology protection measures to protect students from inappropriate access.

 (see next page)

PAGE 7 - IJNDB-R - USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Employee contact system with students, parents, staff and community

- Any contact/communication system used by any employee to conduct school business or notification to students, parents, staff and community must be on the district approved list.

Issued 9/10/96; Revised 10/10/00, 10/9/01, 4/12/05, 11/9/10, 4/12/11, 4/10/12, 10/18/16, 3/10/20