ACCEPTABLE USE POLICY AND ADMINISTRATIVE REGULATIONS

The Superintendent or designee will oversee the District's Acceptable Use Policy.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.

❑ CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work.

No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy.

❑ GENERAL USE

Employees may not move computer equipment or peripheral devices or make modifications to computer hardware or configurations.

Internet use for educational purposes is restricted to the district's network. Any access for said purposes through personal wireless cards or any other personal access device is prohibited.

The use of personal network devices including, but not limited to, routers, switches, firewalls and wireless access points is prohibited. The use of personal equipment such as, but not limited to, laptops, computers, printers, iPads and personal phones is permitted under and in accordance with the BYD guidelines. Problems or complications that arise from the use of these devices are not the responsibility of the district.

❑ FILTERING

The Technology Director and the Technology staff will maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on the District network.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

❑ REQUESTS TO DISABLE FILTER

Users who wish to use a blocked site for bona fide research or other lawful purposes may submit a request to the Instructional Technology Specialist. The ITS will make recommendations to the Technology Director or Network Manager regarding approval or disapproval of disabling the filter for the requested use. The final decision will be made by the Superintendent or the Assistant Superintendent of Administration.

❑ SYSTEM ACCESS

Access to the District's electronic communications system will be governed as follows:

1. Students and District employees will be granted access to the District's system as deemed appropriate. All users will be required to sign a user agreement annually.
2. The District may require that all passwords be changed as needed.
3. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.
4. For access to and policy regarding the use of the district Wi-Fi, please see the BYD Policy.

❑ INDIVIDUAL USER RESPONSIBILITIES/ ONLINE CONDUCT

The following standards will apply to all users of the District's electronic information/communications systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
2. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
3. Communications may not be encrypted so as to avoid security review by system administrators.
4. System users may not use another person's system account for any purpose.
5. Authorization to bypass the content filter is granted solely to specific users and is intended for appropriate educational purposes only. Any other use of the bypass is prohibited. Any bypass of the content filter that is not explicitly granted or authorized by appropriate staff is also prohibited.
6. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
7. No participation in any chat room (or newsgroup) accessed on the Internet is permissible for students or employees.
8. System users must purge electronic mail in accordance with established retention guidelines.
9. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
10. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
11. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
12. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
13. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
14. System users may not waste District resources related to the electronic communications system.
15. System users may not gain unauthorized access to resources or information including, but not limited to, files, pictures, usernames and passwords, or programs.

❑ FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password for any purpose is prohibited.

❑ NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

- Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
- Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
- Pretending to be someone else when sending/receiving messages is considered inappropriate.
- Transmitting obscene messages or pictures is prohibited.
- Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
- Using the network in such a way that would disrupt the use of the network by other users is prohibited.

❑ VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism, as defined above, will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

❑ INTELLECTUAL PROPERTY

All students and employees will:

1. Assume that materials available on the Internet or in other digital resources are protected by copyright unless otherwise labeled. This includes text, graphics, photos, music, videos, and software.
2. Follow Fair Use guidelines when using materials from the Internet or other digital resources in your own work. Follow posted usage policies or ask permission of the original creator, and give proper credit/attribution to the original source.
3. Avoid plagiarism by always giving credit to the original source of ideas you use or works you quote in your own work.

❑ TECHNOLOGY DIRECTOR RESPONSIBILITIES

The technology director for the District's electronic communications system (or campus designee) will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system complete and sign annually an agreement to abide by District policies and administrative regulations regarding such use.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent or designee.
7. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
8. Set limits for data storage within the District's system, as needed.

❑ INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

❑ DISTRICT WEB SITE

The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated Webmaster. The Technology Department will establish guidelines for the development and format of Web pages controlled by the District.

❑ SCHOOL, TEACHER, OR EXTRA-CURRICULAR WEB PAGES

The campus principal will designate the staff member responsible for managing the campus's Web page under the supervision of the ITS. Teachers will be responsible for compliance with District rules in maintaining their class/organization web pages. Any links from a class or organization web page to sites outside the District's computer system must adhere to the district AUP.

❑ TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or Technology Director receives notice of revocation of system privileges or on a future date if so specified in the notice.

❑ DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

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.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.