– SECTION D –
ACCEPTABLE USE OF THE DISTRICT'S ELECTRONIC COMMUNICATIONS SYSTEM

CHILDREN'S INTERNET PROTECTION ACT
Under the Children's Internet Protection Act (CIPA), the District must, as a prerequisite to receiving universal service discount rates, implement certain Internet safety measures and submit certification to the Federal Communications Commission (FCC). *47 U.S.C. 254* [See UNIVERSAL SERVICE DISCOUNTS, below, for details]

Districts that do not receive universal service discounts but do receive certain federal funding under the Elementary and Secondary Education Act (ESEA) must, as a prerequisite to receiving these funds, implement certain Internet safety measures and submit certification to the Department of Education (DOE). *20 U.S.C. 7001* [See ESEA FUNDING, below, for details]

DEFINITIONS
"Harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value. *47 U.S.C. 254(h) (7) (G); 20 U.S.C.6777 (e) (6)*

"Technology protection measure" means a specific technology that blocks or filters Internet access. *47 U.S.C. 254(h) (7)*

INTERNET SAFETY POLICY
The District shall adopt and implement an Internet safety policy that addresses:

1. Access by minors to inappropriate matter on the Internet and the World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including "hacking," and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

47 U.S.C. 254(l)

PUBLIC HEARING
The District shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy. *47 U.S.C. 254(h) (5) (A), (l) (1)*

INAPPROPRIATE FOR MINORS
A determination regarding what matter is inappropriate for minors shall be made by the Board or designee. *47 U.S.C. 254(l) (2)*

TECHNOLOGY PROTECTION MEASURE
In accordance with the appropriate certification, the District shall operate a technology protection measure that protects minors against access to visual depictions that are obscene, child pornography, or harmful to minors; and protects adults against access to visual depictions that are obscene or child pornography. *47 U.S.C. 254(h) (5) (B), (C)*

MONITORED USE
In accordance with the appropriate certification, the District shall monitor the on-line activities of minors. *47 U.S.C. 254(h) (5) (B)*

SECURITY BREACH NOTIFICATION
A district that owns, licenses, or maintains computerized data that includes sensitive personal information shall comply, in the event of a breach of system security, with the notification requirements of Business and Commerce Code 521.053 to the same extent as a person who conducts business in this state. *Local Gov't Code 205.010*

SFDRCISD POLICY CQ (LOCAL)
The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS
Access to the District's Electronic Communications System, computers, the Internet, and other computer resources shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.
4. Has no sexual/inappropriate content

USE BY MEMBERS OF THE PUBLIC
When possible and available and in accordance with the District's administrative regulations, members of the District community may use the District's Electronic Communications Systems, computers, the Internet, other computer resources and software for education or District-related activities, as long as the use:

1. Imposes no measurable cost on the District; and
2. Does not unduly burden the District's computer or network resources.

The equipment, software, and network resources provided through the District are and remain the property of the District. Users of District equipment shall comply with all policies, procedures, and guidelines of the

District and access may be denied to any student, employee, or community member who fails to comply with those policies, procedures, and guidelines.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to District's Electronic Communications System, computers, the Internet, and other computer resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all policies and administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with these policies, regulations, and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

PERSONAL SOFTWARE

Personal software may not be loaded on District computers.

REQUESTING LIMITED OR NO CONTACT WITH A STUDENT THROUGH ELECTRONIC MEDIA

Teachers and other approved employees are permitted by the District to communicate with students through the use of electronic media within the scope of the individual's professional responsibilities. For example, a teacher may set up a social networking page for his or her class that has information related to class work, homework and test. As a parent, you are welcome to join or become a member of such a page.

An employee described above may also contact a student individually through electronic media to communicate about items such as homework or upcoming tests.

If you prefer that your child not receive any one-to-one electronic communications from a district employee, please submit a written request to the campus principal stating this preference.

DISTRICT SOFTWARE

All software used in District computers must be legally licensed. Proper documentation must be maintained.

INTERNET SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms.

FILTERING

Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

MONITORED USE

Electronic mail transmissions and other use of the District's Electronic Communications System by students and employees shall not be considered private. The District reserves the right to monitor access to and use of e-mail, the Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring shall occur at any time to ensure appropriate use and it shall be restricted to individuals specifically designated by the Superintendent.

INTELLECTUAL PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's Electronic Communications System.

As agents of the District, employees shall have limited rights to work they create using the District's Electronic Communications System. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

ELECTRONIC COPYRIGHT LAW

The electronic transmission, distribution, or use of copyrighted materials through the District's Electronic Communications System beyond Fair Use without required citation or written permission by the author is prohibited.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

SFDRCISD ADMINISTRATIVE REGULATION FOR ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

The Superintendent or designee will oversee the District's Electronic Communications System.

The Electronic Communications System is defined as the District's network, servers, computer workstations, telephones, peripherals, applications, databases, library catalog, online resources, internet access, e-mail, online class activities and any other technology designated for use by the District.

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. [See CQ (EXHIBIT E)]

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 will be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy. [See CQ (EXHIBIT F) and policies at FL]

FILTERING

The Superintendent will appoint an Internet Safety committee, to be chaired by the Chief Technology Officer, to select, implement, and 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 computers with Internet access provided by the District.

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

The Internet Safety committee will approve and disapprove requests from users who wish to use a blocked site for bona fide research or other lawful purposes. Appeals shall be made to the **Chief Technology Officer.**

SYSTEM ACCESS

Access to the District's Electronic Communications System will be governed as follows:

1. Students in all grades will be granted access to the District system, as appropriate if an acceptable use form has been signed.
2. District employees will be granted access to the District's system as appropriate and with the approval of the immediate supervisor.
3. A teacher with any class account(s) will be ultimately responsible for use of that student's account.
4. The District will require that all passwords be changed every 120 days with a strong recommendation for every 90 days. Refer to Administrative Regulation TEC-02 for additional password requirements.
5. 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.
6. All users will be required to sign or electronically acknowledge a user agreement annually for issuance or renewal of an account.

TECHNOLOGY SUPERVISION RESPONSIBILITIES FOR STUDENTS

The Superintendent or designees 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 annually complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office and/or online if acknowledgment of receipt was made online.
3. Ensure that employees supervise Internet activity of students who use the District's Electronic Communications System.
4. Ensure that employees provide training to students who use the District's system on the appropriate and safe use of this resource.
5. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
6. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student on-line safety and proper use of the Electronic Communications System.
7. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Director of Technology.
8. Be authorized to establish and enforce a retention schedule for messages on the District e-mail system.
9. Be authorized to establish and enforce a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
10. Set and enforce limits for data storage within the District's system, as needed.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's Electronic Communications Systems:

CONDUCT ON THE SYSTEM

1. The individual in whose name a system account is issued will be responsible at all times for its proper use. Passwords and other information related to system and network access are restricted to that individual and must never be shared with anyone else.
2. System users may not use another person's system account without written permission from a supervising administrator and approved by the Chief Technology Officer, or designee.
3. 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.
4. System users may not disable, bypass, or attempt to disable or bypass a filtering device on the District's Electronic Communications System.
5. Communications may not be encrypted so as to avoid security review or monitoring by system administrators.
6. System users may not gain unauthorized access to resources or information.
7. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
8. 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, telephone numbers, or unauthorized pictures.
9. System users may not engage in harassing, insulting, ostracizing, intimidating, or any other online conduct that could be considered bullying and/or cyberbullying while using any District technology resource, to include the use of any website or software used by the District.
10. Students should never make appointments to meet people whom they meet on-line and if they receive such requests, students must immediately report it to a teacher or an administrator.
11. 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.

12. 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 or loading data from unprotected computers.
13. System users may not send, forward, or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including but not limited to "sexting."
14. System users may not send, forward, or post chain e-mail. Users may not send, forward, or post any messages that are for personal use.
15. System users may not auto-forward District-related e-mail to his or her personal non-District e-mail account. Likewise, non-District related e-mail may not be auto-forwarded to the District e-mail system. When outside of the District, users may access their District-related e-mail through the District provided webmail system.
16. System users may not waste District Electronic Communication System resources (e.g. e-mail spamming, distribution of videos or photos, listening to web radio, etc.).
17. System users may not make any long-distance phone calls without the approval of their supervisor.
18. System users may not send text messages from a District-provided cell phone for non-District purposes.
19. System users must manage electronic mail in accordance with e-mail regulations and established retention guidelines.
20. System users should be mindful that use of school-related electronic mail addresses and fax transmissions might cause some recipients or other readers of that communication to assume they represent the District or school, whether or not that was the user's intention.
21. District-wide e-mail broadcasts must be approved by the Chief Technology Officer.
22. Campus/site-wide e-mail broadcasts must be approved by the campus Principal/Site Administrator.
23. System users may not disconnect or move District computer workstation(s) without first obtaining approval from their campus administrator/department chair/Director. If the District computer workstation(s) require a reconnect to the network and/or configuring, then Technology Services must be contacted. At no time shall users reconfigure District equipment.
24. System users may not connect non-District purchased technology equipment to the Electronic Communications System. Personal laptops are permitted for use by all staff and students at specified campuses. These personal laptops should only be connected to the District's public wireless network called SFDRCISD Wi-Fi.
25. Only District evaluated and approved technology may be purchased and used on the Electronic Communications System.
26. In order to maintain confidentiality of data when using District online applications, users must logout of the application and close the Internet browser of the computer they are using when done.
27. In order to maintain confidentiality of data when using any District applications, in or out of the District, users must take extra precautions to restrict disclosure, access, or viewing of data from people who do not have a need to know (e.g. employees, family, and friends).
28. All users with personal wireless laptops must use the District provided wireless network which is filtered according to the Children's Internet Protection Act (CIPA) requirements. Users are not to use non-District wireless service providers while on District property.
29. Personal wireless laptops are not to be plugged into the wired network. They are only authorized for wireless connectivity.

VANDALISM PROHIBITED (TECHNOLOGY)

Any malicious attempt to harm or destroy District equipment or data 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, downloading, 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]

FORGERY PROHIBITED (TECHNOLOGY)

Forgery or attempted forgery of electronic mail messages and/or signatures 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 is prohibited.

INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION (TECHNOLOGY)

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]

PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS

Limited to educational and District related activities only, participation in chat rooms and newsgroups accessed on the Internet is permissible for students, under appropriate supervision, and for employees.

DISTRICT WEBSITE

The District will maintain a District website 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 website must be directed to the designated Webmaster. The Chief Technology Officer in collaboration with Technology Services will establish guidelines for the development and format of Web pages controlled by the District. Campus web pages will be linked to the District website by the District Webmaster.

No personally identifiable information regarding a student will be published on a website controlled by the District without written permission from the student and the student's parent.

No commercial advertising will be permitted on a website controlled by the District.

SCHOOL OR CLASS WEB PAGES

Schools or classes may publish Web pages that present information about the school or class activities to the District web server upon approval from the campus principal or designee (campus webmaster). The campus principal will designate the staff member responsible for managing the campus' web page. Teachers will be responsible for compliance with the District's Acceptable Use policies and the Web Publishing Guidelines in maintaining their class web pages. Any links from a school or class Web page to sites outside the District's computer system must also be in compliance with the District's Acceptable Use policies and the Web Publishing Guidelines.

STUDENT WEB PAGES

With the approval of the campus principal or designee, students may submit individual Web pages linked to a campus Web page. All material presented on a student's Web page must be related to the student's educational activities and be in compliance with the District's Acceptable Use policies and Web Publishing Guidelines. Student Web pages must include the following notice: *"This is a student Web page. Opinions expressed on this page shall not be attributed to the District."* Any links from a student's Web page to sites outside the District's computer system must also be in compliance with the District's Acceptable Use policies and the Web Publishing Guidelines.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

With the approval of the campus principal, campus extracurricular organizations may submit Web pages linked to a campus Web site. All material presented on the Web page must relate specifically to organization activities and include only staff or student-produced material. The web page must be in compliance with the District's Acceptable Use policies and the Web Publishing Guidelines. The sponsor of the organization will be responsible for compliance with District web development and maintenance rules. Web pages of extracurricular organizations must include the following notice: "*This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District.*" Any links from the Web page of an extracurricular organization to sites outside the District's computer system must receive approval from the campus principal.

PERSONAL WEB PAGES

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.

ELECTRONIC COMMUNICATIONS ETIQUETTE

System users are expected to observe the following etiquette when using the District's Electronic Communications System (e-mail, online communication applications, etc.):

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is inappropriate and prohibited.
4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the computer system or may be in a format unreadable by the recipient.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
7. If a chain letter or an e-mail forward is received, do not continue to forward the message through the District's e-mail system.
8. E-mails containing any discussion or exchange of information about a student's or employee's performance or behavior should not be forwarded to anyone (e.g. parents, other District staff, and non-District staff) without the permission of the originator.
9. Avoid sending e-mail to colleagues or parents that contain personally identifiable information about students or colleagues. An employee shall not reveal confidential information concerning students or colleagues unless disclosure serves lawful professional purposes or is required by law.
10. District wireless equipment should only be connected to an authorized wireless access point (e.g. District, home, hotel) rather than unauthorized access point (e.g. neighbor's access point).

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 District supervisor receives/issues 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.

COMPLAINTS REGARDING COPYRIGHT COMPLIANCE

The District designates the following employee to receive any complaints that copyrighted material is improperly contained in the District network:

Name: Leslie Hayenga
Position: Director of Technology
Address: Raymond Haynes Administration Complex
900 Cantu Rd.
Telephone: (830) 778-4016
E-mail: leslie.hayenga@sfdr-cisd.org