The following exhibits are located in this section:

Exhibit A: Employee Guidelines for Acceptable Use of Technology Resources — 5 pages

Exhibit B: Student Guidelines for Acceptable Use of Technology Resources — 5 pages

Exhibit C: Agreement for Acceptable Use of the Electronic Communications System by a Nonschool User — 2 pages

Exhibit D: Agreement for Electronic Instructional Materials or Technological Equipment — 2 pages

EXHIBIT A

BASTROP INDEPENDENT SCHOOL DISTRICT
EMPLOYEE GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

These guidelines are provided here so that employees are aware of the responsibilities they accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

    a. Use of computers, other technical hardware, computer networks, and software is only allowed when granted permission by the employee's supervisor.

    b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus, as well as on the District's Web site.

    c. Although the District has an Internet safety plan in place, employees are expected to notify their supervisor or the director of technology whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

    d. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the director of technology without discussing it with others.

    e. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.

    f. Employees, upon leaving employment, or upon request from the Superintendent, must return any District-owned equipment or resources in his/her possession.

    g. Employees will be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. [See DH]

2. Unacceptable conduct includes, but is not limited to, the following:

    a. Using the network for illegal activities, including copyright or contract violations, or downloading inappropriate materials, viruses, and/or software, or hacking and host file-sharing software.

    b. Using the network for financial or commercial gain, advertising, proselytizing, or political lobbying.

c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.

d. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Use or possession of hacking software is strictly prohibited.

e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

f. Wasting finite resources, i.e., downloading movies or music for non-educational purposes.

g. Gaining unauthorized access anywhere on the network.

h. Revealing personal information, including but not limited to, the home address or phone number of one's self or another person.

i. Invading the privacy of other individuals.

j. Using another user's account, password, or ID card or allowing another user access to your account, password, or ID.

k. Coaching, helping, observing, or joining any unauthorized activity on the network.

l. Posting anonymous messages or unlawful information on the system.

m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, slanderous.

n. Falsifying permission, authorization of identification documents.

o. Obtaining copies of or modifying files, data, or passwords belonging to other users on the network.

p. Knowingly placing a computer virus on a computer or network.

q. Using personal devices on the District's network, with the exception of approved BYOD devices. [See Part 3: d. Bring Your Own Device]

r. Inappropriately communicating with a student or minor through electronic communication, including but not limited to a cell phone, text messaging, electronic mail, instant messaging, blogging, or other social network communication. [See DH(EXHIBIT)]

3. Acceptable use guidelines are as follows:

   a. General Guidelines:

      (1) All employees will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

      (2) Employees are responsible for their ethical and educational use of the computer online services in the District.

      (3) All policies and restrictions of the District's computer online services must be followed.

      (4) Access to the District's computer online services is a privilege and not a right. Each employee will be required to sign and adhere to the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer online services.

      (5) The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

      (6) When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other education resources.

      (7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses.

      (8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual campus administrator or technology administrator will be considered an act of vandalism and subject to disciplinary action in accordance with Board policy.

   b. Network Etiquette:

      (1) Be polite.

      (2) Use appropriate language.

      (3) Do not reveal personal data (home address, phone number, phone numbers of other people).

      (4) Remember that the other users of the District's computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

      (5) Users should be polite when forwarding e-mail. The intent of forwarding e-mail should be on a need-to-know basis.

c. E-Mail:

(1) E-mail should be primarily used for educational or administrative purposes.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the District's computer online services by employees or any other user will not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail contents are property of the District.

d. Bring Your Own Device:

(1) Employees may bring their own device as part of our Bring Your Own Device (BYOD) program.

(2) Employees may use a personal device in place of (or along with) their district assigned devices if they choose. If the BYOD device is damaged or stolen while on BISD property, the user will not hold BISD liable for the replacement or repair of the device. The user will also be responsible for any data and/or SMS/MMS (texting) charges. BISD will not reimburse users for charges incurred while on BYOD devices. Additionally, BISD will not provide technical support for BYOD devices.

(3) Employees may join the BISD guest wireless service with their BYOD device upon agreeing to install a policy key. This will ensure your device meets all security and filtering requirements.

4. Consequences:

a. The employee, in whose name a system account and/or computer hardware is issued, will be responsible at all times for its appropriate use.

b. Noncompliance with the guidelines published here, in the Student Code of Conduct, and in Board policy CQ(LOCAL) may result in suspension or termination of technology privileges and disciplinary actions. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District.

c. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications using District equipment and network access is governed by the Texas Open Records Act, therefore, when legally requested, proper authorities will be given access to their contents.

BASTROP ISD ACCEPTABLE USE AGREEMENT SHEET

Employee Name (print) _____

School/Location _____

I have read the Employee Acceptable Use Guidelines for Bastrop ISD. I agree to follow the rules contained in these guidelines. I further understand that electronic mail transmissions and other use of the electronic communications systems, including the Internet, are not private and may be monitored at any time by the District staff to ensure appropriate use, as defined by the Acceptable Use Guidelines. I understand that violations can result in disciplinary action such as denial of access privileges, change in employment status, appropriate legal action, and/or termination of employment.

Employee Signature _____

Date _____

EXHIBIT B

BASTROP INDEPENDENT SCHOOL DISTRICT
STUDENT GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

These guidelines are provided here so that students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:
    a. Student use of computers, other technology hardware, software, and computer networks, including the Internet, is only allowed when supervised or granted permission by a staff member.

    b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the District's Website.

    c. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

    d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Unacceptable conduct includes, but is not limited to the following:

    a. Using the network for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, hacking, and host file-sharing software.

    b. Using the network for financial or commercial gain, advertising, proselytizing, or political lobbying.

    c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.

    d. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Use or possession of hacking software is strictly prohibited.

    e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

    f. Wasting finite resources, i.e., downloading movies or music for non-educational purposes.

    g. Gaining unauthorized access anywhere on the network.

h. Revealing personal information, including but not limited to, the home address or phone number of one's self or another person.

i. Invading the privacy of other individuals.

j. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

k. Coaching, helping, observing, or joining any unauthorized activity on the network.

l. Posting anonymous messages or unlawful information on the system.

m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, stalking, or slanderous.

n. Falsifying permission, authorization, or identification documents.

o. Obtaining copies of or modifying files, data, or passwords belonging to other users on the network.

p. Knowingly placing a computer virus on a computer or network.

q. Using personal devices on the District's network, with the exception of approved BYOD devices. [See Part 3: d. Bring Your Own Device]

3. Acceptable use guidelines for the District's network computer online services are as follows:

   a. General Guidelines:

      (1) Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

      (2) Students are responsible for their ethical and educational use of the computer online services in the District.

      (3) All policies and restrictions of the District's computer online services must be followed.

      (4) Access to the District's computer online services is a privilege and not a right. Each employee, student, and/or parent will be required to sign the Acceptable Use Policy Agreement and adhere to the Acceptable Use Guidelines in order to be granted access to District computer online services.

      (5) The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

      (6) When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other education resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's Student Code of Conduct booklet.

(9) Any parent wishing to restrict his or her children's access to any District computer online services will provide this restriction request in writing to the principal. Parents will assume responsibility for imposing restrictions only on their own children.

b. Network Etiquette:

(1) Be polite.

(2) Use appropriate language.

(3) Do not reveal personally identifiable information or data (home address, phone number, phone numbers of other people) or contact unknown individuals.

(4) Remember that the other users of the District's computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

(5) Users should be polite when forwarding e-mail. The intent of forwarding e-mail should be on a need-to-know basis.

c. E-Mail:

(1) E-mail should be used primarily for educational or administrative purposes.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the District's computer online services by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail contents are property of the District.

d. Bring Your Own Device:

(1) Students may bring their own device as part of our Bring Your Own Device (BYOD) program.

(2) Students may use a personal device in class for instructional use with teacher permission. If the BYOD device is damaged or stolen while on BISD property, the user will not hold BISD liable for the replacement or repair of the device. The user will also be responsible for any data and/or SMS/MMS (texting) charges. BISD will not reimburse users for charges incurred while on

BYOD devices. Additionally, BISD will not provide technical support for BYOD devices.

(3) Students may join the BISD guest wireless service with their BYOD device upon agreeing to install a policy key. This will ensure your device meets all security and filtering requirements.

4. Consequences are as follows:

   a. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

   b. Noncompliance with the guidelines published here, in the Student Code of Conduct, and in Board policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to consequences of Board Policy and the Student Code of Conduct. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District.

   c. Electronic mail, network usage, and all stored files will not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.

   d. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Open Records Act; therefore, proper authorities will be given access to their content.

BASTROP ISD ACCEPTABLE USE AGREEMENT

Student Section

Student Name (print) _____ Grade _____

School _____

I have read the Student Acceptable Use Guidelines. I agree to follow the rules contained in this policy. If I violate the rules, I may lose my access privilege to the District's computer online services and may face disciplinary action.

_____ _____

Student Signature Date

Parent Section

I have read the Student Acceptable Use Guidelines. I understand that the Internet is a world-wide group of hundreds of thousands of computer networks. I agree that the Bastrop Independent School District does not control the content of these Internet networks. I understand that if my child violates the Acceptable Use Guidelines, his or her access privilege to the District's computer online services may be revoked and may be subject to disciplinary action. The Bastrop Independent School District has my permission to give network and Internet access to my child. I understand that my child will maintain this privilege as long as procedures described in the District's Acceptable Use Guidelines are followed.

I also grant permission for examples of my child's schoolwork to be published on the World Wide Web as an extension of classroom studies, provided that the home address, home phone number, student's last name, or a close-up photograph is not included.

Note: While the District will use filtering technology to restrict objectionable material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use. Parents who do not want their child to have Internet access and/or have their schoolwork published on the Web should submit this request in writing annually to their child's principal. While the District will attempt to restrict access, it is ultimately the responsibility of the parent to ensure his or her child does not violate this request.

_____ _____

Parent or Guardian Signature Date

_____

Parent name (print)

EXHIBIT C

BASTROP INDEPENDENT SCHOOL DISTRICT

AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM BY A NONSCHOOL USER

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that you read the District's policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

RULES FOR APPROPRIATE USE

You will be assigned an individual account, and you are responsible for not sharing the password for that account with others.

You will be held responsible at all times for the proper use of your account, and the District may suspend or revoke your access if you violate the rules.

Remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.

1. INAPPROPRIATE USES

    a. Using the system for any illegal purpose.

    b. Disabling or attempting to disable any Internet filtering device.

    c. Encrypting communications to avoid security review.

    d. Borrowing someone's account without permission.

    e. Downloading or using copyrighted information without permission from the copyright holder.

    f. Intentionally introducing a virus to the computer system.

    g. Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

h. Wasting school resources through improper use of the computer system.

i. Gaining unauthorized access to restricted information or resources.

2. CONSEQUENCES FOR INAPPROPRIATE USE

a. Suspension of access to the system;

b. Revocation of the computer system account; or

c. Other legal action, in accordance with applicable laws.

I understand that my computer use is not private and that the District will monitor my activity on the computer system.

I have read the District's electronic communications system policy and administrative regulations and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the Bastrop Independent School District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

Name (Print) _____

Signature _____

Home address _____

Date _____ Home phone number _____

EXHIBIT D

AGREEMENT FOR ELECTRONIC INSTRUCTIONAL MATERIALS OR TECHNOLOGICAL EQUIPMENT

In consideration for the District permitting me to use electronic instructional materials or technological equipment for personal business off school property or outside a school-sponsored event, I assume full financial responsibility for usage of such items to pay for any repairs and/or replace the Equipment if it is damaged, stolen, misplaced, or for any other reason not returned. I agree that Bastrop ISD may deduct money from my pay, not to exceed the Replacement Value, to cover the cost of repairing or replacing the Equipment that I may damage (other than normal wear and tear), lose, fail to return, or take without appropriate authorization during my employment. All use will be in accordance with applicable District policies, administrative regulations, and this agreement form. [See policies CQ and DH and provisions on the use of electronic media in the employee handbook.]

If the equipment is lost or stolen, the Superintendent or designee may reduce or eliminate my liability for loss or theft if (i) a police report is filed immediately and (ii) the Superintendent or designee does not find that the loss or theft resulted from my own wrongful or negligent acts or omissions. Such determinations shall be made on a case-by-case basis. I understand that the equipment should not be left unattended.

I also understand that the District recommends that I obtain appropriate insurance for the equipment to cover loss, damage, or destruction. [See DG(LEGAL)]

This document acknowledges my possession of the following Equipment and assumption of financial responsibility for the Equipment usage off school property or outside of a school-sponsored event. I acknowledge that Bastrop ISD has not required that I enter into this agreement as a condition of my employment with Bastrop ISD. I further acknowledge that Bastrop ISD may request the return of the Equipment at any time, and I will be required to return the Equipment within one business day after Bastrop ISD has made such a request. The term "Equipment" as used in this Agreement shall mean the technology equipment described below:

Description	Make	Model	Model #	Service Tag and /or Serial #

***I understand that this user agreement must be renewed each school year.**

Employee Name (Print) _____ Date _____

Employee's signature _____