See the following pages for forms that may be used by the District regarding the use of its technology resources:

Exhibit A: Spring Branch ISD Employee Agreement for Responsible Use of the District's Technology Resources — 7 pages

Exhibit B: Agreement for Responsible Use of the Spring Branch ISD's Technology Resources by a Nonschool User — 3 pages

Exhibit C: Spring Branch ISD Acceptable Use Policy for Electronic Services for Students – 3 pages

Exhibit D: Spring Branch ISD Technology Resources Opt-Out Form

EXHIBIT A

SPRING BRANCH ISD EMPLOYEE AGREEMENT FOR RESPONSIBLE USE OF THE DISTRICT'S TECHNOLOGY RESOURCES

GOVERNMENT LAW AND DISTRICT POLICIES

Employees will use computers in conformity with laws of the United States and the state of Texas. Violations include, but are not limited to, the following:

1. Criminal Acts–These include, but are not limited to, "hacking" or attempting to access computer systems without authorization, harassing e-mail, cyberbullying, cyberstalking, child pornography, vandalism, and/or unauthorized tampering with computer systems.
2. Libel Laws–Publicly defaming people through either published (or the publishing of) material on the Internet, e-mail, and the like.
3. Copyright Violations–Copying, selling, or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), engaging in plagiarism (using others' words or ideas as your own).
4. Personal Information–Unauthorized disclosure, use, and dissemination of personal information regarding minors.

It is important that you read the applicable District policies, administrative regulations, and this agreement form. [See policies CQ and DH, and provisions on use of electronic media in the employee handbook.]

Please contact the District's Technology Compliance Officer at (713) 251-2312 if you have questions or need help understanding this material.

The following guidelines apply to all District networks, e-mail accounts, devices connected to the District's networks, and all District-owned devices used on or off school property, whether connected to the District's network or connected through a personal data plan or other means of access.

Additionally, the District prohibits harassment through electronic means regardless of the device used, the network used, or the location of use. [See District policies DH, DIA, and FFH.]

Inappropriate use of the District's technology resources may result in revocation or suspension of the privilege of using these resources, as well as other disciplinary or legal action, in accordance with applicable District policies, administrative regulations, and laws.

EMPLOYEE ACCESS

You are being given access to the following technology resources:

- A District e-mail account
- A cloud-based (online) document storage and collaboration space (ex: Google Apps for Education)

- District computer hardware, software, and printers on your school campus
- District networks, including document storage space
- District-owned technology resources for use at home
- District-filtered Internet access

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may accidentally see some material you find objectionable. Though the District uses 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 and to report misuse.

If you are being issued a District-owned technology device that can be used off campus, you will be given additional materials addressing the proper use, care, and return of these devices.

All individuals are responsible for the management of computer resources and are accountable for their actions relating to computer resources security. Individuals using computer resources are expected to know and comply with District policies and procedures. An employee may use only the user IDs and passwords assigned to him or her for the purposes intended and may not share or disclose these passwords. Failure on the part of an individual to comply may result in disciplinary and/or legal action including suspension without pay or termination of the employee or his or her contract.

Use of any electronic communication service implies that the employee accepts the responsibility to comply with the policies. The District's purpose for the use of e-mail and Internet resources is to advance and promote education with the intention of assisting in the collaboration and exchange of information. The District's electronic communication systems, including its network access to the Internet, are primarily for administrative and instructional purposes. Personal use of e-mail and the Internet is a privilege, not a right. Limited personal use of the system is permitted if the use:

- Imposes no tangible cost to the District;
- Does not unduly burden the District's technology resources or personnel; and
- Has no adverse effect on job performance or on a student's academic performance.

Electronic mail transmissions and other use of the electronic communication systems are not private and are automatically monitored at all times to ensure appropriate use.

General Guidelines

- All participants will conduct themselves in a responsible, ethical, and polite manner accessing only those resources appropriate for kindergarten–grade 12.
- Personal use of e-mail and the Internet should be restricted to reasonable periods of time such as coffee and lunch breaks.

- Accessing, posting, or sharing any racist, sexist, threatening, obscene, or otherwise objectionable material is strictly prohibited.
- E-mail and the Internet should not be used for any personal monetary interests or gain.
- Employees should not subscribe to mailing lists or services that are not educational publications.
- Employees are not permitted to store or print personal e-mail messages or personal information obtained via the Internet.
- Risks to information resources must be managed at all levels. Data essential to critical District functions must be protected from loss, contamination, or destruction.
- Only those employees or officials expressly authorized to speak to the media or public on behalf of the District may represent the District in such communications via e-mail messages.

Copyrighted Software

Employees are expected to comply with the national software piracy laws. Failure on the part of an individual to comply will result in disciplinary action up to and including suspension without pay or termination of the employee or a contract. A person may be subjected to civil or criminal legal sanctions when a violation occurs. It is the responsibility of all personnel to report any suspected or confirmed violations of this exhibit to technology services or appropriate management.

RESPONSIBILITY FOR THE USE OF TECHNOLOGY IN THE DISTRICT

1. Passwords are private. Employees will not allow others to use their account name and password and will not try to use that of others.
2. Employees will be polite and will use appropriate language in e-mail messages, virtual learning environments, online postings, and other digital communications with others and will refrain from using profanity, vulgarities, or any other inappropriate language as determined by administrators.
3. Employees will not use computers, handheld computers, digital audio players, cell phones, personal digital devices, or the Internet to send or post hate or harassing mail, pornography, or discriminatory or derogatory remarks about others, or to engage in harassment or other antisocial behaviors.
4. Employees will not communicate directly with any student between the hours of 10:00 p.m. and 6:30 a.m. Exceptions include any extracurricular/curricular activities, field trips, and emergency situations that may require contact before 6:30 a.m. or after 10:00 p.m.
5. Employees will refrain from inappropriate communication with a student. Factors considered in assessing whether the communication is inappropriate include, but are not limited to:

    a. Nature, purpose, timing, and amount of communication;

b. The subject matter of the communication;

c. Whether the communication was made openly or was attempted to be concealed;

d. Whether the communication was sexually explicit; and

e. Whether the communication could be interpreted as soliciting sexual contact or a romantic relationship.

6. Administrators may require staff to include an administrator or designee to be copied on texts sent to students.

7. Employees represent the District in all online activities. Employee participation on social networking Web sites such as MySpace and Facebook should not reflect negatively on students, employees, or the District. Employees will be held responsible for how they represent the District on the Internet.

8. District employees will not use personal social networking sites (e.g., Facebook, MySpace, and the like) to interact with students. Employees must create a separate instructional group or site (e.g., Facebook, MySpace, and the like) for academic/educational networking with students.

9. Masquerading, spoofing, or pretending to be someone else is forbidden. This includes, but is not limited to, sending out e-mails, creating accounts, or posting messages or other online content (e.g., text, images, audio, or video) in someone else's name as a joke.

10. Employees will use technology resources responsibly and will not retrieve, save, or display hate-based, offensive, or sexually explicit material using any of the District's computer resources. Employees are responsible for not pursuing material that could be considered offensive.

11. Employees will use technology resources productively and responsibly for educational purposes and will avoid using any technology resource in such a way that would disrupt the activities of other users.

12. Employees will refrain from attempting to bypass or circumvent District security settings or Internet filters and from interfering with the operation of the network by installing illegal software or Web-based services and software not appearing on the approved District software list.

13. Vandalism is prohibited. This includes, but is not limited to, modifying or destroying equipment, programs, files, or settings on any computer or other technology resource.

14. Employees will refrain from the use of or access to files, software, or other resources owned by others without the owner's permission and will use only those school network directories that are designated for their use.

15. District administrators will deem what conduct is inappropriate use if such conduct is not specified in this agreement.

16. Employees will abide by all Internet safety guidelines.

17. Employees will save only District business-related work and information to devices and data storage folder(s) provided by the District.

18. Employees will not distribute personal information about students or other employees without District authorization; this includes, but is not limited to, personal addresses and telephone numbers.

19. Employees will comply with the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), and any other applicable law or policy regarding records retention and confidentiality of student and District records.

20. Employees will maintain the confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.

21. Before use on a District device or for a District purpose, digital subscriptions, online learning resources, online applications, or any other program will be approved by Technology Services. District staff should not accept terms and conditions or sign user agreements on behalf of the District without preapproval from the purchasing director or designee.

22. Copies of potentially sensitive or confidential District records should not be sent, viewed, or stored using an online application not approved by the District.

23. District-owned devices and personal devices that allow access to District e-mail or potentially sensitive student or employee records will be password protected.

24. Employees will immediately report any suspicious behavior or other misuse of technology to their supervisor or an administrator.

25. Employees will not use e-mail or Web sites to engage in or encourage illegal behavior or to threaten school safety.

26. Employees are not to post or transmit pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of 18.

USE OF PERSONALLY OWNED DEVICES

With District approval, employees may use approved personal devices for accessing the Internet through the guest network for instructional purposes. Employees will assume responsibility for any technical issues related to their personal devices. The District is not responsible for installation of software, peripheral devices, or any loss or damage of personal devices.

- Personal devices that allow access to District e-mail or potentially sensitive student or employee records must be password protected.
- Confidential information should not be downloaded onto or stored on personal devices.

EDUCATION, SUPERVISION, AND MONITORING

It will be the responsibility of all members of the District to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with the Children's Internet Protection Act (CIPA).

CONSEQUENCES FOR VIOLATION OF THIS AGREEMENT

Violation of this agreement will result in the following consequences:

- Suspension of access to the District's technology resources;
- Revocation of the account; and
- Other disciplinary or legal action, in accordance with the District's policies and applicable laws.

REPORTING VIOLATIONS

An employee must immediately report any known violation of the District's applicable policies, Internet safety plan, or acceptable use guidelines to his or her supervisor.

An employee must report to his or her supervisor instances of anyone sharing personally identifying information, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

RETURN OF TECHNOLOGY RESOURCES AND RECORDS

Upon leaving employment, or upon request from the Superintendent, an employee must return any District-owned equipment or resources in his or her possession.

An employee must also return any records, written or electronic, to the District for records retention if the employee has reason to believe he or she is retaining the sole copy of a record subject to records retention requirements. The employee must destroy (delete or shred) any other confidential records remaining in his or her possession.

CONSEQUENCES FOR VIOLATION OF THIS AGREEMENT

I understand that my use of the District's technology resources is not private and that the District will monitor my activity.

I have read the District's technology resources policy, associated administrative regulations, and this user agreement and agree to abide by their provisions. In consideration for the privilege of using the District's technology resources, I hereby release the 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, these resources, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

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

Signature of Employee Date

Printed Name of Employee

Disclaimer

These guidelines apply to stand-alone computers as well as to computers connected to the network/Internet. The District makes no warranties of any kind, whether expressed or implied, for the services it is providing and is not responsible for any damages suffered by users. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its negligence, user errors, or omissions. The District is not responsible for phone/credit card bills or any other charges incurred by users. Use of any information obtained via the network/Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. 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 communication systems.

EXHIBIT B

AGREEMENT FOR RESPONSIBLE USE OF THE
SPRING BRANCH ISD'S TECHNOLOGY RESOURCES BY A NONSCHOOL USER

You are being given access to the District's technology resources, meaning electronic communication systems and electronic equipment. It is important that you read the applicable District policies, administrative regulations, and agreement form. Please contact the District's technology compliance officer at (713) 251-2312 if you have questions or need help understanding this material.

The following guidelines apply to all District networks, e-mail accounts, devices connected to the District's networks, and all District-owned devices used on or off school property, whether connected to the District's network or connected through a personal data plan or other means of access.

Inappropriate use of the District's technology resources may result in suspension or revocation of the privilege of using these resources, as well as other legal action, in accordance with applicable laws.

As a user of the District's technology resources, based on your access level, you may have access to:

- A variety of servers, databases, files, libraries, and resources;
- The Internet and other electronic information systems/networks, which can be used to communicate with schools, colleges, organizations, and individuals around the world; and
- Shared electronic equipment, which may have stored temporary Internet and electronic files of other users.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may accidentally access content and material that you find objectionable. While the District uses 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 and to report misuse.

RULES FOR RESPONSIBLE USE

- You will be held responsible at all times for the proper use of District technology resources, and the District may suspend or revoke your access if you violate the rules.
- You will be assigned an individual account, and you are responsible for not sharing the password for that account with others.

INAPPROPRIATE USES

- Using the resources for any illegal purpose.

- Accessing the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communication systems in violation of the law or District policy.
- Damaging electronic communication systems or electronic equipment, including knowingly or intentionally introducing a virus to a device or network, or not taking proper security steps to prevent a device or network from becoming vulnerable.
- Disabling or attempting to disable any Internet filtering device.
- Encrypting communications to avoid security review.
- Using someone's account without permission.
- Pretending to be someone else when posting, transmitting, or receiving messages.
- Attempting to read, delete, copy, modify, or interfere with another user's posting, transmittal, or receipt of electronic media.
- Using resources to engage in conduct that harasses or bullies others.
- Sending, posting, or possessing materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including cyberbullying and "sexting."
- Using e-mail or Web sites to engage in or encourage illegal behavior or to threaten school safety.
- Using inappropriate language such as swear words, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- Violating others' intellectual property rights, including downloading or using copyrighted information without permission from the copyright holder.
- Posting, transmitting, or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Posting or transmitting pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of 18.
- Wasting school resources through improper use of the District's technology resources, including sending spam.
- Gaining unauthorized access to restricted information or resources.

CONSEQUENCES FOR INAPPROPRIATE USE

- Suspension of access to the District's technology resources;
- Revocation of the account; or
- Other legal action, in accordance with applicable laws.

REPORTING VIOLATIONS

- You must immediately report any known violation of the District's applicable policies, Internet safety plan, or responsible use guidelines to the technology coordinator.
- You must report to the technology coordinator requests for personally identifying information, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

I understand that my use of the District's technology resources is not private and that the District will monitor my activity.

I have read the District's technology resources policy [see CQ(LOCAL)], associated administrative regulations, and this user agreement and agree to abide by their provisions. In consideration for the privilege of using the District's technology resources, I hereby release the 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, these resources, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

Signature: _____

Home address: _____

Date: _____ Home phone number: _____

EXHIBIT C

SPRING BRANCH INDEPENDENT SCHOOL DISTRICT

ACCEPTABLE USE POLICY FOR ELECTRONIC SERVICES FOR STUDENTS

Spring Branch Independent School District (SBISD) strongly believes in the educational value of electronic services and recognizes the potential to support curriculum and student learning by facilitating resource sharing, innovation, and communication.

Access to the Internet allows students to explore thousands of libraries, databases, museums, and other repositories of information. Families should be aware that some material accessible via the Internet may contain items that are inappropriate, inaccurate, or potentially offensive. While the school's intent is for students to use electronic resources for constructive educational goals, students may find ways to access other materials. The District believes the benefits to students from using electronic services to access information resources and for collaboration exceed the disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Therefore, the District supports and respects each family's right to deny electronic services to their student by submitting an "opt-out" form to the school's principal [see below].

Authorized student use of information resources must be consistent with the educational purposes for which these resources have been provided. The use of SBISD electronic services is to assist students in completing educational activities and should be used in a manner that enhances educational experiences and complies with SBISD policies. All student users must adhere to the provisions of this Acceptable Use Policy as a condition for continued use of the SBISD network. This policy must be followed anytime there is a connection to the District's wired or wireless network via any electronic device. SBISD reserves the right to monitor any user's online activities. Users should have no expectation of privacy regarding their use of SBISD property, including the network, Internet access, files, text, chat room conversations, and e-mail.

Internet Safety

In compliance with the Children's Internet Protection Act ("CIPA"), Spring Branch Independent School District is required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them. Furthermore, each campus educates students on cyberbullying, appropriate online behavior, and social networking as required by Broadband Data Improvement Act.

1. SBISD has implemented filtering and/or blocking software to restrict access to Internet sites containing pornography, obscene depictions, or other materials harmful to minors under 18 years of age, to the extent practicable, while using its network. This control also applies to other forms of communication such as e-mail, chat rooms, social network-

ing sites, instant messaging, and the like. However, no software is foolproof, and there is still a risk a user may be exposed to a site or message containing such materials.

2. The student's parent or guardian is responsible for supervising and monitoring all device usage that occurs outside the SBISD network.
3. Students will not reveal personal information, including name, home address, telephone number, photos, and the like on the Internet. Students are advised to never access, keep, or send anything that they would not want the general public to see.
4. Students will not meet in person with anyone they have met only online via the Internet.
5. The user is personally responsible for his or her actions in accessing and utilizing the school's device resources.
6. Students must abide by all laws, regulations, the Student Code of Conduct, Acceptable Use Policy, and other related SBISD security policies.

Privacy

The Family Educational Rights and Privacy Act ("FERPA") is a federal law that protects the privacy of student education records. Under FERPA, parents or eligible students have the right to inspect and review the student's education records maintained by the school. Students and qualified parents can view certain educational records of the student online through Skyward Family Access. These records are safeguarded through all available means and access will be restricted to parents/guardians and the student through the use of user names and passwords.

Acceptable Actions

SBISD students may use the network and electronic services provided by SBISD to pursue educational activities. Students will learn how Internet resources can provide valuable educational information. Students will be expected to follow accepted rules of network etiquette. These rules include, but are not limited to the following:

- Be courteous and respectful. Do not send or display offensive messages or pictures.
- Use appropriate language in any type of communication. No profane, abusive, or impolite language will be used to communicate nor should materials be accessed that are not in line with the rules of school behavior.
- Keep personal information such as logins, passwords, addresses, and phone numbers confidential.
- Use electronic services for educational purposes only.
- If you encounter materials that violate the rules of appropriate use, disconnect immediately and notify an adult.

Unacceptable Actions

Improper use of electronic services provided by SBISD is prohibited. Be prepared to be held accountable for your actions and the loss of privileges if this Acceptable Use Policy is violated. In addition to the paragraph below labeled “Penalties for Improper Use,” the SBISD Student Code of Conduct addresses the consequences for violations. Actions that constitute unacceptable use include, but are not limited to the following:

- Do not use a device to harm other people or their work.
- Do not damage the device or the network in any way.
- Do not interfere with the operation of the network by installing software, shareware, or freeware, including the alteration of any controls designed to provide Internet safety or alteration of SBISD’s default device image.
- Do not violate copyright laws or participate in any criminal activities punishable by law.
- Do not view, send, or display offensive messages or pictures.
- Do not share your password with another person or offer access to any person via your account.
- Do not reveal your personal address or phone numbers or those of other students or colleagues, including the completion of profile data.
- Do not waste limited resources such as disk space or printing capacity.
- Do not distribute advertisements, solicitations, commercial ventures, or political lobbying.
- Do not trespass in another's folders, work, or files.
- Do not pursue internal or external “hacking”, use anonymous e-mail sites, spread viruses, initiate spam, or attempt to access inappropriate material.

All SBISD students are granted access to all electronic services available. If the parent/guardian DOES NOT want the student to have access to electronic services, please complete and submit the opt-out form and access will be denied.

Penalties for Improper Use

The use of the network is a privilege, not a right, and may be revoked if abused. Misuse, damage, or vandalism of SBISD technology resources may also lead to disciplinary and/or legal action, including suspension, expulsion, or criminal prosecution by governmental authorities.

Disclaimer

SBISD makes no guarantee about the quality of services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from the use of its network. Any charge accrued to the user of SBISD’s network are borne by the user. Statements by the user on the Internet are from the author’s individual point of view and do not represent the views of SBISD, its employees, or members of the Board of Education.

Student and parental/guardian signatures on the Student Code of Conduct represent consent to conform to the Acceptable Use Policy.

EXHIBIT D

Spring Branch ISD Technology Resources Opt-Out Form

_____	_____	_____
Student Name	Grade	Campus

The Technology Responsible Use Policy guidelines are located in the Student Handbook. Circle your preference: ***Unless I indicate No below I am granting permission.**		
I grant permission for my child to access SBISD technology resources and Internet.	Yes	No
I grant permission for my child to use district-issued email.	Yes	No
Parent/Guardian Signature:		
Printed Parent/Guardian Name:	Date:	

Parent/Guardian Permission to Online Publication

The district's teaching and learning practices include creating and publicly publishing on the Web examples of student work such as writing pieces, photographs of classroom learning activities, videos, drawings, participation in educational networks, classroom blogs, etc.

***Unless I indicate No below I am granting permission.**

Circle your preference:		
I grant permission to publicly publish my child's: • First name last initial (elementary) • First name last name (secondary) • Voice • Work • Photograph/video	Yes	No
Parent/Guardian Signature:		
Printed Parent/Guardian Name:	Date:	