See the following for forms related to use of District technology resources:

Exhibit A: Letter to Parents Regarding Use of Online Technology Resources — 1 page

Exhibit B: Student Agreement for Acceptable Use of the District’s Technology Resources — 6 pages

Exhibit C: Employee Agreement for Acceptable Use of the District’s Technology Resources — 4 pages

Exhibit D: Board Member Agreement for Acceptable Use of the District’s Technology Resources — 4 pages

Exhibit E: Agreement for Acceptable Use of the District’s Technology Resources by a Nonschool User — 3 pages

Exhibit F: Staff Request for Approval of Technology Resources — 1 page

Exhibit G: Data Breach Prevention and Response Plan — 3 pages

EXHIBIT A

LETTER TO PARENTS REGARDING USE OF ONLINE TECHNOLOGY RESOURCES

Dear Parents:

Your child has access to a variety of technology resources through the District, including online applications for use on or off campus. Resources such as online encyclopedias, instructional videos, interactive tutorials, and many other applications offer teachers, students, and families an unprecedented variety of tools to enhance effective teaching and learning.

All websites, digital subscriptions, and technology tools made available to students through the District have been vetted by the District's technology team for quality, appropriateness, online security, and data privacy. The specific resources available to your child will depend on your child's age and grade level and are outlined in the attached Student Agreement for Acceptable Use of the District's Technology Resources.

Additionally, the District contracts with certain providers of online educational services to provide District services and functions, including essential instructional and logistical programs such as the District's online grade book and the online lunch account management system. Where personally identifiable student information is implicated, service providers act as District officials and access only the information needed to perform the contracted service. These outside parties are under the District's direct control with respect to the use and maintenance of student data. A list of such services and the nature and type of student information used is available at http://www.sfdr-cisd.org/student-page.

It is important that you and your child read the enclosed District policy and student agreement form and discuss these requirements together.

Sincerely,

____
Principal or Technology Director

EXHIBIT B

STUDENT AGREEMENT FOR ACCEPTABLE USE OF THE DISTRICT'S TECHNOLOGY RESOURCES

You are being given access to the District-provided technology resources listed below.

With this educational opportunity comes responsibility. It is important that you and your parents read the applicable District policies, administrative regulations, and agreement form and contact Les Hayenga, SFDRCISD Technology Director at (830) 778-4016 if you have questions. Inappropriate use of the District's technology resources may result in revocation or suspension of the privilege to use these resources, as well as other disciplinary or legal action, in accordance with the Student Code of Conduct and applicable laws.

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 bullying or harassment through electronic means regardless of the device used, the network used, or the location of use. [See District policies FFH and FFI]

You are being given access to the following technology resources:

- A District e-mail account.
- A District e-mail account, including access to cloud-based (online) document storage and collaboration space (*Google Apps for Education, for instance).*
- District computer hardware, software, and printers on your school campus.
- District networks, including document storage space.
- Access to 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 run across areas of adult content and some material you (or your parents) 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 responsible use.

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

RULES FOR RESPONSIBLE USE

- District technology resources are primarily for instructional and educational purposes. Limited personal use is allowed only if the rules in this agreement are followed, and the use does not interfere with school work.

- If you are issued your own account and password, you must not share your account information with another person.
- You must remember that people who receive e-mail or other communication from you through your school account might think your message represents the school's point of view.
- You must always keep your personal information and the personal information of others private. This includes name, address, photographs, or any other personally identifiable or private information.
- Students will not download or sign up for any online resource or application without prior approval from their teacher or other District administrator.
- Elementary students in grades PK-5th grade will not sign up for individual accounts, but will use a District or classroom account, as applicable.
- When communicating through e-mail or other electronic means, you must use appropriate language and etiquette as you would when communicating face to face. Always be respectful.
- You must be sure to acknowledge the work and ideas of others when you reference them in your own work.
- You must immediately report any suspicious behavior or other misuse of technology to your teacher or other campus administrator.
- 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.

INAPPROPRIATE USES

The following are examples of inappropriate uses of technology resources that may result in loss of privileges or disciplinary action:

- Using the resources for any illegal purpose, including threatening school safety.
- Accessing the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communications system 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 or bypass any Internet filtering device.
- 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 material that constitutes cyberbullying and "sexting."
- Using inappropriate language such as cursing, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- Posting personal information about yourself or others, such as addresses, phone numbers, or photographs without permission, or responding to requests for personally identifiable information or contact from unknown individuals.
- Making appointments to meet in person people met online. If a request for such a meeting is received, it should be immediately reported to a teacher or administrator.
- Violating others' intellectual property rights, including downloading or using copyrighted information without permission from the copyright holder.
- Wasting school resources through the improper use of the District's technology resources, including sending spam.
- Downloading unauthorized applications or software or gaining unauthorized access to restricted information or resources.

REPORTING VIOLATIONS

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

STUDENT

Name: ________________ Grade: _______ School: _______________

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, including the District's guidelines for responsible online behavior and use of social networking websites. I understand that violation of these provisions may result in suspension or revocation of access to the District's technology resources or other disciplinary action in accordance with the Student Code of Conduct.

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

Student's signature:

____

Date: ____________________

PARENT

As the parent or guardian of this student, I have read the SFDRCISD technology resources policy, associated administrative regulations, and this user agreement. In consideration for the privilege of my child 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 child's use of, or inability to use, these resources, including, without limitation, the type of damage identified in the District's policy and administrative regulations.

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

I understand that the District uses certain cloud-based (online) applications, meaning applications such as *Google docs or Skyward* that allow authorized individuals to access student information, including assignments and grades, through the Internet for school-related purposes. A list of online applications and the nature and type of student information used is available at http://www.sfdr-cisd.org/student-page.

□ I give permission for my child to access the District's technology resources, including District-approved online applications, and certify that the information contained on this form is correct.

Parent's signature:

____

Date: ____________________

ADDENDUM ADDRESSING STUDENT USE OF PERSONAL TELECOMMUNICATIONS OR OTHER ELECTRONIC DEVICES FOR INSTRUCTIONAL PURPOSES WHILE ON CAMPUS BRING YOUR OWN DEVICE (BYOD) POLICY

The District permits use of personal telecommunications or other electronic devices by students for instructional purposes while on campus.

RULES FOR RESPONSIBLE USE

- You may use your personal electronic device for instructional purposes only as authorized by your teacher.
- When using the device for instructional purposes while on campus, you must use the District's wireless Internet services and are prohibited from using a personal wireless service. Any attempt to bypass the District's filter will result in loss of privileges and disciplinary action as required by the Student Code of Conduct.
- When accessing the District's technology resources using your personal device, you must follow the District's technology resources policy and associated administrative regulations, including the acceptable use agreement you signed for access to the District's technology resources.
- When not using the device for instructional purposes while on campus, you must follow the rules and guidelines for noninstructional use as published in the student handbook.

CONSEQUENCES FOR INAPPROPRIATE USE

- Suspension of access to the District's technology resources;
- Revocation of permission to use personal electronic devices for instructional purposes while on campus; or
- Other disciplinary or legal action, in accordance with the Student Code of Conduct and applicable laws.

The District is not responsible for damage to or loss of devices brought from home.

STUDENT

I wish to use the following telecommunications or other electronic device for instructional purposes while on campus:

____

____

Name: ________________________ Grade: ________School: ____________________

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

I understand that my personal electronic device may be searched by District administrators in accordance with policy FNF.

I have read the applicable District policies, associated administrative regulations, and this user agreement regarding the District's technology resources and use of student-owned electronic devices and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access and/or suspension or revocation of permission to use my personal electronic device for instructional purposes while on campus.

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

Student's signature: ___________________ Date: ______________________

PARENT

□ I do not give permission for my child to use his or her personal electronic device(s) at school for instructional purposes while on campus.

I have read the applicable District policies, associated administrative regulations, and this user agreement regarding the District's technology resources and use of student-owned electronic devices. In consideration for the privilege of my child 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 child's use of, or inability to use, these resources, including, without limitation, the type of damage identified in the District's policies and administrative regulations.

I understand that my child's use of the District's technology resources, including the District's wireless Internet services, is not private and that the District will monitor my child's activity.

I understand that my child's personal electronic device may be searched by District administrators in accordance with policy FNF.

□ I give permission for my child to use his or her personal electronic device(s) at school for instructional purposes while on campus.

Parent's signature: ___________________ Date: ______________________

EXHIBIT C

EMPLOYEE AGREEMENT FOR ACCEPTABLE USE OF THE DISTRICT'S TECHNOLOGY RESOURCES

You are being given access to the District-provided technology resources listed below. 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 Les Hayenga, SFDRCISD Technology Director at (830) 778-4016 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.

You are being given access to the following technology resources:

- A District e-mail account.
- A District e-mail account, including access to cloud-based (online) document storage and collaboration space (*Microsoft Outlook and Google Apps for Education, for instance).*
- District computer hardware, software, and printers on your school campus.
- District networks, including document storage space.
- Access to 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 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.

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.

RULES FOR RESPONSIBLE USE

- You will be assigned an individual account for access to approved District technology resources, and you are responsible for not sharing your password or other account information with others.
- District technology resources are primarily for instructional and educational purposes. Limited personal use is allowed only if the rules in this agreement are followed and the use does not interfere with your assigned duties.
- You must 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.
- You must maintain the confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.
- You must remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.
- When communicating through e-mail or other electronic means, you must use appropriate language and etiquette as you would when communicating face to face. Always be respectful.
- Only authorized District staff may communicate with District students through electronic means, including social media, e-mail, and text messaging. If you are unsure whether or not you are authorized to communicate with a student through electronic means, ask your supervisor. [See DH]
- Before use on a District device or for a District purpose, digital subscriptions, online learning resources, online applications, or any other program must be approved by the SFDRCISD Technology Director. District staff should not accept terms and conditions or sign user agreements on behalf of the District without preapproval.
- Copies of potentially sensitive or confidential District records should not be sent, viewed, or stored using an online application not approved by the District.
- You must immediately report any suspicious behavior or other misuse of technology to your supervisor or other campus administrator.
- 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.

INAPPROPRIATE USES

- Using the resources for any illegal purpose, including threatening school safety.
- Accessing the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communications system 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 or bypass 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 others.
- Sending, posting, or possessing materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including material that constitutes prohibited harassment and "sexting."
- Using inappropriate language such as cursing, 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 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 disciplinary or legal action, in accordance with the District's policies and applicable laws.

REPORTING VIOLATIONS

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

RETURN OF TECHNOLOGY RESOURCES AND RECORDS

- Upon leaving employment, or upon request from the Superintendent, you must return any District-owned equipment or resources in your possession.
- You must also return any records, written or electronic, to the District for records retention if you have reason to believe you are retaining the sole copy of a record subject to records retention requirements. You must destroy (delete or shred) any other confidential records remaining in your possession.

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: __________________ Date: ____________

I understand that in consideration for the District permitting me to use electronic instructional materials or technological equipment for personal business, I assume financial responsibility for usage of such items off school property or outside of a school-sponsored event. All use will be in accordance with 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]

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

Technology resource(s) issued:	*Maximum financial responsibility incurred in the event of loss, damage, or destruction:

*Financial responsibility may be less than this amount based on the nature of the damage.

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

Signature: __________________ Date: ____________

EXHIBIT D

BOARD MEMBER AGREEMENT FOR ACCEPTABLE USE OF THE DISTRICT'S TECHNOLOGY RESOURCES

You are being given access to the District-provided technology resources listed below. It is important that you read the applicable District policies, administrative regulations, and this agreement form. [See policies BBI and CQ]

Please contact the Superintendent 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.

You are being given access to the following technology resources:

- A District e-mail account.
- A District e-mail account, including access to cloud-based (online) document storage.
- District computer hardware, software, and printers.
- District networks, including document storage space.
- Access to 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 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.

If you are being issued a District technology device, you will be given additional materials addressing the proper use, care, and return of these devices.

RULES FOR RESPONSIBLE USE

- You will be assigned an individual account for access to approved District technology resources, and you are responsible for not sharing the password or other account information with others.

- District technology resources are to be used primarily for official duties, but some limited personal use is permitted.
- You must comply with the District's record management program, the Texas Open Meetings Act, the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), and campaign laws.
- You must maintain confidentiality of student and District records.
- You must maintain the confidentiality of health or personnel information concerning District employees and colleagues, unless disclosure serves lawful professional purposes or is required by law.
- You must remember that people who receive e-mail from you with a District address might think your message represents the District's point of view.
- Before use on a District device, digital subscriptions, online applications, or any other program requiring the user to accept terms of service or a user agreement must be approved by the Superintendent.
- Copies of potentially sensitive or confidential District records should not be sent, viewed, or stored using an online application not approved by the District.
- 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.

INAPPROPRIATE USES

- Using the resources for any illegal purpose, including threatening school safety.
- Accessing the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communications system 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 or bypass any Internet filtering device. Requests to disable a filtering device should be made to the Superintendent.
- 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 others.

- Sending, posting, or possessing materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including material that constitutes prohibited harassment or "sexting."
- Using inappropriate language such as cursing, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- 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.
- Violating others' intellectual property rights, including downloading or using copyrighted information without permission from the copyright holder.
- 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 acceptable use guidelines to the Superintendent.
- You must report to the Superintendent 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 the Board, you must return any District-owned equipment or resources in your possession.
- You must also return any records, written or electronic, to the District for records retention if you have reason to believe you are retaining the sole copy of a record subject to records retention requirements. You must destroy (delete or shred) any other confidential records remaining in your possession.

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 policies [see policies BBI and CQ], 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: ___________________ Date: _____________

Home Address: ___________________ Home/Mobile phone number: _____________

EXHIBIT E

AGREEMENT FOR ACCEPTABLE USE OF THE DISTRICT'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 this agreement form. Please contact Les Hayenga, Director of Technology at (830) 778-4016 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.

You are being given access to the following technology resources:

- District computer hardware, software, and/or printer.
- 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 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 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.
- If you are assigned an individual account, you are responsible for not sharing the password or other account information with others.

INAPPROPRIATE USES

- Using the resources for any illegal purpose, including threatening school safety.
- Accessing the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communications system 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 or bypass 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 material that constitutes cyberbullying and "sexting."
- Using inappropriate language such as cursing, 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 acceptable use guidelines to Les Hayenga, SFDRCISD Technology Director at (830) 778-4016.

- You must report requests for personally identifiable information, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal to the technology coordinator.

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.

Signature: ___________________ Date: ____________

Home Address: ___________________ Home/Mobile phone number: ____________

EXHIBIT F

STAFF REQUEST FOR APPROVAL OF TECHNOLOGY RESOURCES

Before use in the classroom, use with students, or administrative use, all online learning resources, online applications, digital subscription services, and other programs or technology applications requiring the user to accept terms of service or a user agreement must be approved by the SFDRCISD Technology Director.

To request to use such an online resource or technology application other than a District-approved resource, please complete and submit the following form.

Name: ____

Position: ____________________________________ (*ex. teacher*)

Date: ____________

If the resource will be used by students, which grade(s):

____

1. Give name and description of the technology resource you are requesting to use. If you are requesting an online resource, please include a link to the resource.

   ____

   ____

   ____

2. Describe how you plan to use the requested resource. What information, if any, will be shared? Who will have access to the resource? If for use by students, will students need to sign up for an account or download an application? Is parental permission required by the application before use by a student?

   ____

   ____

   ____

For Office Use Only

☐ Approved for use

  ☐ Additional parent notification and permission required.

  ☐ No additional notifications or permissions required.

☐ Not approved for use at this time.

  ☐ Reason:

  ____

EXHIBIT G

DATA BREACH PREVENTION AND RESPONSE PLAN

The following data breach prevention and response plan includes guidelines for preventing a data breach and for responding quickly and effectively after a breach occurs.

The District's technology coordinator is responsible for annually reviewing this plan and updating the guidelines as needed.

1. Security Breach Prevention

□ Maintain and update the breach response team contact list: □ Check that contact information is accurate. □ Redistribute the updated list as needed.	Quarterly
□ Review the District's information systems and keep records of locations and systems that house personally identifiable information and other sensitive information. □ Ensure confidential information is stored on a secure server that is accessible only with a password or other security protection. □ Keep and update records of all persons with access to District servers through personal or District-issued mobile devices and laptops and ensure each device is password protected and encrypted, as applicable. □ Ensure that District-maintained cloud-based applications that use or maintain student or staff data are compliant with the Family Educational Rights and Privacy Act (FERPA), the Children's Internet Protection Act (CIPA), and other federal and state law. □ Review requests from professional staff members for use of additional online educational resources, including review of the terms of service or user agreements to ensure compliance with District standards, and applicable law. □ Compile a list of third-party vendors with access to sensitive information, including the types of information and uses of the information. □ Issue a reminder to all relevant parties to secure sensitive paper records; to password protect records stored on thumb drives, external hard drives, and laptops; and to dispose of records in accordance with the District's records retention requirements.	Quarterly

☐	Review third-party vendor contracts: ☐ Coordinate with the business office to ensure that vendor contracts for cloud-based applications that use or maintain student or staff data are compliant with FERPA, CIPA, and other federal and state law. ☐ Ensure contracts include breach notification.	Annually
☐	In conjunction with the records retention officer, ensure archived data meets industry standards and legal requirements for secure storage and review data storage and disposal protocols.	Annually
☐	Update local security measures, including: ☐ System passwords, including a list of District employees with administrator access to information systems ☐ Antivirus software (should update automatically) ☐ Firewalls ☐ Data backup procedures ☐ Data encryption procedures ☐ Data and records disposal best practices	Quarterly
☐	Monitor systems for data loss.	Continually
☐	Conduct trainings with students, staff members, Board members, and others as needed on privacy and security awareness and District protocols for storing, accessing, retaining, and disposing of records.	Annually

2. Breach Response Team

Name	Position	Contact information	Responsibility during breach
Les Hayenga	Technology Coordinator/Instructional Technology Director	Phone: (830) 778-4016 E-mail: leslie.hayenga@sfdr-cisd.org	Notify team Identify affected records
Rene Luna	Director of Communications	Phone: (830) 778-4164 E-mail: rene.luna@sfdr-cisd.org	Coordinate notification and communications plan

Robert Schulman	Legal Counsel	Phone: (210) 538-5385 E-mail: rschulman@slh-law.com	Analyze legal implications and advise team related to litigation risks and notification requirements

3. Responding to a breach:

Upon notification that a security breach may have occurred, Les Hayenga, SFDRCISD Technology Director, will immediately notify the breach response team and:

□ Validate the data breach;

□ Determine the scope of the breach;

□ Notify law enforcement, if needed;

□ Coordinate the breach response team and ensure team handles responsibilities in accordance with the nature and severity of the breach, including determining whether notification of affected individuals is appropriate and, if so, how best to provide the notification;

□ Gather and maintain all documents related to the breach; and

□ Analyze information to determine the cause of the breach (internal cause, third-party breach) and take measures to address and remediate.