Table of Contents

Exhibit A—Irving Independent School District Acceptable Use Policy for Employees

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

For the purpose of this agreement, terms such as “employee,” “you,” “your,” and “I” refer to the Irving Independent School District employee. Terms such as “we,” “us,” and “District” refer to Irving Independent School District.

1. You agree that the expectations are as follows:

    a. Your use of computers, other electronic devices, computer networks, and software is only allowed when granted permission by the employee’s supervisor.

    b. Copyright compliance is the law. All students and employees of the District are required to follow copyright guidelines. Guidelines are listed near the campus copy machine and on the District website.

    c. Although the District has an internet safety plan in place, you are expected to notify your supervisor or the cybersecurity team whenever you come across information or messages that are inappropriate, dangerous, threatening, or make you feel uncomfortable.

    d. If you identify or know about a security problem, you are expected to convey the details to your supervisor or the systems security administrator without discussing it with others.

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

    f. You are held to the same professional standards in your public use of electronic media as you are for any other public conduct. If your use of electronic media violates state or federal law or District policy or interferes with your ability to effectively perform your job duties, you are subject to disciplinary action, up to and including termination of employment. [See DH]

2. You agree unacceptable conduct includes, but is not limited to, the following:

    a. Using the network for illegal activities, including downloading copyright, license, or contract material or downloading inappropriate materials, malware, software, hacking utilities, and/or peer-to-peer 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. Unauthorized use or possession of hacking software is strictly prohibited.

e. Causing congestion on the network or interfering with the work of others, e.g., forwarding chain letter emails, sending broadcast messages to lists or individuals, or unauthorized or noncurricular use of online video, music, or streaming content.

f. Wasting finite resources, e.g., downloading movies or music for noneducational purposes.

g. Gaining unauthorized access anywhere on the District's network or District devices.

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

i. Using authorized access to invade the privacy of other individuals or to access confidential information outside of business needs.

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

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

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

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

n. Making an audio or video recording of any student, teacher, or administrator without prior permission from the subject.

o. Using technology resources to bully, harass, or tease other people.

p. Falsifying permission, authorization, of identification documents.

q. Unauthorized capturing, forwarding, or altering of files, data, stored data, or data in transmission, belonging to other users or District devices on the network.

r. Knowingly installing or introducing malware on the District network or a District device.

s. Using personal computing devices on the District's network, with the exception of approved mobile devices for District-approved programs.

t. Using active listening devices such as but not limited to Alexa, Siri, or Google Home on District premises.

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

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

(3) Access to the District's online services is a privilege and not a right. Each employee is required to sign and adhere to this acceptable use policy in order to be granted access to District computer online services.

(4) The use of any District 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.

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

(6) Transmission of any material that violates 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 malware.

(7) Any attempt to alter data, the configuration of an electronic device, 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 online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

c. Email Etiquette:

(1) Users should be polite when forwarding email. The intent of forwarding email should be on a need-to-know basis.

(2) Email should be primarily used for educational or administrative purposes.

(3) Email transmissions, stored data, transmitted data, or any other use of the District's 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.

(4) All email and all email contents are property of the District.

4. Consequences:

a. The employee is responsible for the appropriate use of all assigned system accounts and/or electronic devices.

b. Noncompliance with the guidelines published here or 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 email 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.

Irving ISD Acceptable Use Agreement

Employee Name *(print)* _____

School/Location _____

I have read the Irving Independent School District Acceptable Use Policy for Employees. I understand and agree to follow the rules contained in these guidelines. I further understand that electronic mail transmissions and other use of the digital resources, 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 Policy. 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—Irving Independent School District Acceptable Use Policy for Students

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

For the purpose of this agreement, terms such as “you,” “your,” “parent(s),” and “I” refer to the Irving Independent School District student and/or parent. Terms such as “we,” “us,” and “District” refer to Irving Independent School District.

1. You agree that the expectations are as follows:

    a. Your use of computers, other electronic devices, software, and computer networks, including the internet, is only allowed when supervised or granted permission by a staff member.

    b. Copyright compliance is the law. All students and employees of the District are required to follow copyright guidelines. Guidelines are listed near the campus copy machine and on the District website.

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

    d. If you identify or know about a security problem, you are expected to convey the details to your teacher, counselor, or campus administrator without discussing it with other students.

2. You agree that unacceptable conduct includes, but is not limited to, the following:

    a. Using the network for illegal activities, including downloading copyright, license, and/or contract material or downloading inappropriate materials, malware, software, hacking utilities, and/or peer-to-peer 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. Unauthorized 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 letter emails, broadcast messages to lists or individuals, or unauthorized or noncurricular use of online video, music, or streaming content.

f. Wasting finite resources, e.g., downloading movies or music for noneducational purposes.

g. Gaining unauthorized access anywhere on the District's network.

h. Revealing personal information, including but not limited to the home address or phone number of oneself 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 card.

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

l. Posting anonymous messages or unlawful information on any 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. Making an audio or video recording of any student, teacher, or administrator without prior permission from the subject.

o. Using technology resources to bully, harass, or tease other people.

p. Falsifying permission, authorization, or identification documents.

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

r. Knowingly installing or introducing malware on a District device or the District network.

s. Unauthorized capturing, forwarding, or altering of files, data, stored data, or data in transmission, belonging to other users or District devices on the network.

t. Using active listening devices such as but not limited to Alexa, Siri, or Google Home on District premises.

3. Acceptable use guidelines for the District's network 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 online services in the District.

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

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

(5) The use of any District 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 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 malware.

(8) Any attempt to alter data or the files of another user without the consent of the owner or any attempt to alter the configuration of any electronic device will be considered an act of vandalism and subject to disciplinary action in accordance with the District's Student Code of Conduct.

(9) Any parent wishing to restrict his or her children's access to any District online services will provide this restriction request in writing to the principal. Parents will assume responsibility for imposing restrictions 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 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 email. The intent of forwarding email should be on a need-to-know basis.

c. Email Etiquette:

(1) Email should be used primarily for educational or administrative purposes.

(2) Users should be polite when forwarding email or using reply-all. The intent of forwarding email or using reply-all should be on a need-to-know basis. Additional reply-all restrictions may be set by a campus principal or department supervisor.

(3) Email 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.

(4) All email and all email contents are property of the District.

4. Consequences are as follows:

a. The student is responsible for the appropriate use of all assigned system accounts and/or electronic devices.

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 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 are not 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 email and network communications are governed by the Texas Open Records Act; therefore, proper authorities will be given access to their content.

Irving ISD Acceptable Use Agreement

Student Section

Student Name *(print)* _____ Grade _____

School _____

I have read the Irving Independent School District Acceptable Use Policy for Students. I agree to follow the rules contained in this policy. If I violate the rules, I may lose my privilege to access the District's online services and may face disciplinary action.

Student signature _____ Date _____

Parent section

I have read the Irving Independent School District Acceptable Use Policy for Students. I agree it is my responsibility to follow this Acceptable Use Policy. I agree that if my child violates the Irving Independent School District Acceptable Use Policy for Students, his or her access privilege to the District's online services may be revoked and may be subject to disciplinary action. The Irving Independent School District has my permission to give network and internet access to my child. I agree that my child will maintain this privilege as long as procedures described in the Irving Independent School District Acceptable Use Policy for Students are followed.

I agree that the internet is a world-wide group of hundreds of thousands of computer networks. I agree that the Irving Independent School District does not control the content of these internet networks. While the District will use content filtering technology to restrict objectionable material, I agree that it is not possible to successfully filter and restrict all objectionable material.

I 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.

If I do not want my child to have internet access and/or have their schoolwork published on the internet, I should submit this request in writing to their principal annually. While the District will attempt to restrict internet access, it is ultimately my responsibility to ensure my child does not violate this request. I understand that restricting access to the internet also restricts my child's learning opportunity since many of the student resources are digital.

Parent or Guardian signature _____

Parent name *(print)* _____

Date _____

Home address _____

Phone: _____

Exhibit C—Irving Independent School District Acceptable Use Policy for Guest Users

You are being given access to the District's digital resources. Through these resources, you will be able to communicate with other schools, colleges, organizations, and people around the world through the internet. 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 access to the District's digital resources.

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.

1. You agree that the expectations are as follows:

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

    b. 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.

    c. You will be held to the same professional standards in your public use of electronic media as you are for any other public conduct. If your use of the digital resources violates state or federal law or District policy or interferes with your ability to effectively perform your job duties (function in the District), you are subject to disciplinary action, up to and including termination of employment/contract/relationship with the District. Remember that people who receive email from you with a school address might think your message represents the school's point of view.

2. You agree unacceptable conduct includes, but is not limited to, the following:

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

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

f. Causing congestion on the network or interfering with the work of others, e.g., chain letter emails, or broadcast messages to lists or individuals, or unauthorized or noncurricular use of online video, music, or streaming content.

g. Knowingly installing or introducing malware on a District device or the District network.

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

i. Making an audio or video recording of any student, teacher, or administrator without prior permission from the subject.

j. Using technology resources to bully, harass, or tease other people.

k. Wasting school resources through improper use of the digital resources.

l. Gaining unauthorized access to restricted information, resources, or networks.

m. Capturing, forwarding, or altering files, data, stored data, or data in transmission belonging to other District devices on the network.

n. Using active listening devices such as, but not limited to, Alexa, Siri, and Google Home.

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

3. Consequences for inappropriate use:

a. Suspension of access to the system;

b. Revocation of the digital resource privilege; or

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

Irving Independent School District Acceptable Use Agreement for Guest Users

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

I have read this Acceptable Use Policy for Guest Users and agree to follow the rules in this policy. In consideration for the privilege of using the District's digital resources and in consideration for having access to the public networks, I hereby release the Irving 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 Use Policy for Guest Users.

Name *(print)* _____

Signature _____

Home address _____

Phone number _____

Date _____

Exhibit D—Release Form for the Electronic Display of Original Work

I, _____, give my permission for my work to be publicly displayed electronically and to be produced by the District. The work to be displayed is:

_____

_____

Student's or employee's signature _____

Date _____

Signature of student's parent _____

Date _____

Home phone number _____