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 _____