Agreement for Acceptable Use of Technology Resources by Interim Employees

As an interim employee, you are being given access to the District's technology resources. **The technology resources are defined as the District's network (including wireless access), servers, computer workstations, peripherals, applications, databases, online resources, Internet access, electronic mail, digitized information, telecommunication devices, and any other technology designated for use by students, including all new technologies as they become available.**

The use of DISD technology resources is a privilege, not a right, and should be treated as such. DISD firmly believes that the value of providing information, interaction, and research capabilities far outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

In accordance with the Children's Internet Protection Act (CIPA), Duncanville Independent School District educates staff and students regarding appropriate online behavior to insure Internet safety and has deployed filtering technology and protection measures to restrict access to inappropriate content such as those that are illegal, harmful, or contain potentially offensive information. [See policy CQ] While every effort is made to provide the most secure and optimal learning environment, it is not possible to absolutely prevent access (accidental or otherwise) to inappropriate content.

The technology resources are defined as the District's network (including both wired and wireless access), servers, computer workstations, peripherals, applications, databases, online resources, Internet access, electronic mail, digitized information, telecommunication devices, and any other technology designated for use by students, including all new technologies as they become available.

Please acknowledge receipt and understanding of the District's Acceptable Use Agreement by completing and returning this document.

ACCEPTABLE USE

- You must comply with all district policies, guidelines and Federal and State law. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary action. Should you have questions about computer use and data management can contact the Director of Technology.
- Some users may be assigned an individual account for hardware and Internet access, and are responsible for maintaining the security of your account password. You may not share your password with others.
- The account is to be used mainly for purposes related to educational programs, school operations, and performance of job responsibilities, but some limited personal use is permitted. [See Policy CQ]
- Users shall report any security breach or inappropriate websites not being filtered to the system administrator using the Website Block/Unblock Request, accessed through the Staff Portal. [See policy DH.]
- Users are responsible for proper care of district equipment [See Policy CQ] and report malfunctioning equipment in a timely manner to the Technology Help Desk. [See Policy CL]
- Users must make reasonable effort to ensure that district equipment is not stolen from unmonitored classrooms or vehicles
- Users are responsible for proper care and use of district Infrastructure. Unauthorized Infrastructure equipment (routers, switches, access points, personal computing, and/or digital appliances) must be vetted via district technology department prior to granting access prior to accessing district Infrastructure.

INAPPROPRIATE USE

- Attempting to or harming equipment, materials or data.

- Using the system for any illegal purpose, including by not limited to gambling.
- Disabling or attempting to disable any Internet filtering device.
- Encrypting communications to avoid security review.
- Borrowing someone's account without permission.
- Forgery or pretending to be someone else when sending or receiving messages.
- Attempting to send anonymous messages of any kind.
- Violation of copyright laws is prohibited.
- Intentionally introducing a virus to the computer system.
- Submitting, publishing or displaying any defamatory, cyber bullying, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private. [See Policy DF]
- Wasting school resources through improper use of the computer system.
- Gaining unauthorized access to restricted information or resources including, not limited to, opening, viewing, using, or deleting files belonging to another system user without permission.
- Using the network for individual financial gain, political or commercial activity.
- Posting personal information or images about students or others (i.e., addresses, phone numbers, and pictures).
- Broadcasting or uploading digital content without expressed written consent from the district.

PROFESSIONAL INTERNET POSTING/ELECTRONIC MEDIA

The district reserves the right to remove, disable, and provide feedback regarding professional social media sites that do not adhere to district policy or standards of operation. If an employee's use of electronic media interferes with the user's ability to effectively perform his or her job duties, the user is subject to disciplinary action, up to and including termination of employment. [See Policy DH (Exhibit)]

The following guidelines will apply for any employee who uses electronic media for professional purposes:

- Professional sites should include language identifying the sites as professional social media sites of the district or campus.
- Users should exercise caution, sound judgment, and common sense when using professional social media sites. The employee should regularly monitor professional social media sites to protect the school community.
- When establishing professional social media sites, supervisors and employees should consider the intended audience for the site and consider the level of privacy assigned to the site, specifically, whether the site should be a private network or a public network.
- Any media inquiries received via professional social media sites should be referred to the district's Communications Department in compliance with the district's Media Guidelines.

PERSONAL INTERNET POSTING/ELECTRONIC MEDIA

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (email), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, LinkedIn). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications.

As role models for the district's students, users are responsible for their public conduct even when they are not acting as district staff members. Users will be held to the same professional standards in their public use of electronic media as they are for any other public conduct. [See Policy DH.]

If an interim employee uses of electronic media interferes with his/her ability to effectively perform his or her job duties, the staff member is subject to disciplinary action, up to and including termination of employment. [See Policy DH (Exhibit).] If a user wishes to use a social network site or similar media for personal purposes, he/she is responsible for the content on the his/her page, including content added by the staff member, his/her friends, or members of the public who can access the staff member's page, and for Web links on the staff member's page. The user is also responsible for maintaining privacy settings appropriate to the content.

The following guidelines will apply for any employee who uses electronic media for personal purposes:

- The interim employee's use of electronic media for personal purposes should impose no tangible cost on the District; should not unduly burden the District's technology resources; and should have no adverse effect on a user's job performance or on a student's academic performance. [See Policy CQ]
- If an Internet posting makes it clear that the author works for the District, it should include a simple and visible disclaimer such as, "these are my personal views and not those of the District." When posting your point of view, you should neither claim nor imply you are speaking on the District's behalf, unless you are authorized in writing by the Superintendent or his designee, the Chief Communications Officer.
- The employee shall not use the district's logo or other copyrighted material of the district without express, written consent.
- The user is prohibited from knowingly communicating with students through a personal social network page; the staff member must create a separate social network page ("professional page") for the purpose of communicating with students.
- The user shall not use the district's logo or other copyrighted material of the district without express, written consent.
- The user continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, even when communicating regarding personal and private matters, regardless of whether the staff member is using private or public equipment, on or off campus. These restrictions include:
    - Confidentiality of student records. [See Policy FL]
    - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. [See Policy DH (EXHIBIT)]
    - Confidentiality of district records, including educator evaluations and private e-mail addresses. [See Policy GBA]
    - Copyright law [See Policy CY]
    - Prohibition against harming others by knowingly making false statements about a colleague or the school system. See Policy DH (EXHIBIT).

See Use of Electronic Media with Students, below, for regulations on staff communication with students through electronic media.

Agreement for Acceptable Use of Technology Resources by Interim Employees

USE OF PERSONAL ELECTRONIC DEVICES

The District is not responsible for any damaged, lost, or stolen electronic device. The District is not responsible for personal property used to access District computers or networks or for District-provided Internet access on personal learning devices. The District will not be responsible for any consequential damages or unauthorized financial obligations resulting from District-provided access to the Internet.

USE OF ELECTRONIC MEDIA WITH STUDENTS
Policy DH

A certified or licensed staff member, or any other staff member designated in writing by the superintendent or a campus principal, may communicate through electronic media with students who are currently enrolled in the district. The interim employee must comply with the provisions outlined below. All other staff are prohibited from communicating with students who are enrolled in the district through electronic media.

An interim employee is not subject to these provisions to the extent the staff member has a social or family relationship with a student. For example, a staff member may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the staff member's child, or a member or participant in the same civic, social, recreational, or religious organization.

The following definitions apply for the use of electronic media with students:

- Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, LinkedIn). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications.
- Communicate means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by a staff member that is not targeted at students (e.g., a posting on the staff member's personal social network page or a blog) is not a communication: however, the staff member may be subject to district regulations on personal electronic communications. See Personal Use of Electronic Media, above. Unsolicited contact from a student through electronic means is not a communication.
- Certified or licensed employee means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the staff member to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An interim employee who uses electronic media to communicate with students shall observe the following:

- The staff member shall limit communications to matters within the scope of the staff member's professional responsibilities(e.g., for classroom teachers, matters relating to class work, homework, and tests; for a staff member with an extracurricular duty, matters relating to the extracurricular activity.)
- The interim employee is prohibited from knowingly communicating with students through a personal social network page; the staff member must create a separate social network page ("professional page")

for the purpose of communicating with students. The staff member must enable administration and parents to access the staff member's professional page.

- Interim employees are responsible for monitoring appropriate student use and report any violations. [See Policy CQ]
- The interim employee shall not communicate directly with any student between the hours of 7:00 pm and 7:00 am. A staff member may, however, make public posts to a social network site, blog, or similar application at any time. The staff member does not have a right to privacy with respect to communications with students and parents. The staff member continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, including:

    - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. [See Policies CPC and FL]
    - Copyright law [See Policy CY]
    - Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [See Policy DF]
    - Upon request from administration, a staff member will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the staff member uses to communicate with any one or more currently-enrolled students.
    - Upon written request from a parent or student, the staff member shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

An interim employee may request an exception from one or more of the limitations above by submitting a written request to his or her immediate supervisor and receiving approval.

DATA SECURITY

As part of your duties, you may have access to confidential information such as student social security numbers. Caution must be taken to insure this data is not exposed to those without an educational need to know. A data file that contains confidential information could be at risk for inadvertent release, and can damage the financial, professional or emotional futures of others, thus this information must be handled appropriately. [See Policy CQ]

- Limit data exports to only the necessary information on the required people.
- Do not leave data files in an unsecure location such as an unattended automobile.
- Access to confidential information should be given on an as needed basis. If you are able to access confidential information that you do not need, you are required to report it to the manager of that data system.
- Be very cautious in transporting data files. Data transported on flash drives or external drives can be lost easily.
- Cloud based storage systems such as Google Drive and Dropbox are also susceptible to leaks especially if users do not correctly configure sharing permissions. Therefore public web-based file sharing tools should not be used to store confidential information.
- Data files containing confidential information that are leaving the district via email or on media, must be encrypted.

- Users must comply with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student and district records.

CONSEQUENCES FOR INAPPROPRIATE USE

Improper or unethical use may result in disciplinary actions consistent with district policy, if appropriate, and state and federal laws. This may also require restitution for costs associated with system restoration, hardware or software costs.

AGREEMENT FOR ACCEPTABLE USE

As a user of the Duncanville ISD technology resources, I hereby agree to comply with the user agreement and expectations outlined in this document, as well as the staff handbook and District policy.

- I understand that any computer I use is not private and that the District will monitor my activity on the computer system.
- I understand that all users of district Internet and technology should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.
- I understand that using someone else's login is a violation of the Acceptable Use Agreement.
- I have read the Duncanville ISD's Technology Resource Agreement and agree to abide by its provisions. In consideration for the privilege of using the District's technology resources and in consideration for having access to the public networks, 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, the system, including, without limitation, the type of damages identified in the District's policy.
- I realize that I am responsible for the monitoring of network use by students under my supervision. I will immediately report any violations of the Acceptable Use Agreement to the campus principal/direct supervisor and Technology Leadership.