INTRODUCTION TO DUESD TECHNOLOGY DEPARTMENT

Network Privileges

All employees who sign the Acceptable Use Policy (AUP) have a network login and password. Access is available from workstations based upon whether the employee works in the classroom or as administrative support. As the AUP indicates, the email account is restricted to business use. Internet access is filtered by legal requirements. Certain attachments are also restricted to protect the network from viruses and other malicious software.

Data Storage

All data is stored on network drives which are backed up daily; no data is stored on the local C: drive. If necessary, a technician may re-image a workstation which would destroy any data stored locally. Each user has a P: drive to hold private work data. This drive is not accessible by other users. There is also an S: drive for shared data. Folders in the shared drive are available for access by increasingly more District users as they move from Site to District. Depending upon where the file is saved, it becomes available across the network to anyone else who belongs to the group. Only group members have access to the named folder.

Security

Internet and email filtering is in place, as well as antivirus software; however, no filter is perfect. It is expected that employees use discretion in accessing the Internet to prevent access to inappropriate web sites. In order to pass data from home to school and back, there are several ways to proceed. Flash drives, CDRs, and Google Docs/Drive are acceptable, as are most email attachments. Most graphic attachments are prohibited.

Software Availability

District-standard productivity software is available on the network. All software must be installed by Technology staff due to such issues as strict observance of copyright restrictions and minimizing software conflicts.

Admonition

Please refrain from passing around spam emails to other employees via the District's email system or placing any personal files such as family event pictures and videos, personal music files, etc., on the network. These items use up storage and bandwidth that are needed for daily operations. In addition, please remove old or unused files in your P: and Shared drive locations. The District reserves the right to remove any files it deems unnecessary at its discretion.

DELANO UNION ELEMENTARY SCHOOL DISTRICT
ELECTRONIC ON-LINE SERVICES
RULES OF INTERNET ETIQUETTE “NETIQUETTE”

- Be Polite. Never send, or encourage others to send, abusive messages.

- Use Appropriate Language. Remember that you are a representative of not only yourself but also your school on a publicly accessible system. You may be alone with your computer, but what you say and do can be viewed globally! Never swear, use vulgarities, or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

- Privacy. Remember that revealing your own phone number and address can result in unwanted intrusions of your privacy and should be viewed in the same light as a public listing in a telephone directory. Users shall have no expectation of privacy and understand that the District has the right to monitor and examine all system activities to ensure proper use of the system.

- Electronic Mail. Electronic mail (E-Mail) is not guaranteed to be private. Messages relating to or in support of illegal or unethical activities must be reported to the District.

Recommended Practices

- Use accurate and descriptive titles for your articles and subject lines for your e-mail. Tell people what it is about before they read it.
- Get the most appropriate audience for your message, not the widest. Avoid posting and bulk mailing of large messages.
- Remember that if you post to multiple groups, specify all groups in a single message.
- Be brief. Fewer people will bother to read a long message.
- Minimize spelling errors and make sure your message is easy to understand and read.
- Forgive the spelling and grammatical errors of others.
- Remember that humor and satire are very often misinterpreted.
- Post only to groups you know.
- Cite references for any facts you present.
- Keep signatures brief.
- Remember that all network users are human beings. Don't "attack" correspondents; persuade them with facts.

Delano Union School District

Board Policy

Employee Use Of Technology

BP 4040
Personnel

The Governing Board recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting district and school operations; and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use district technology primarily for purposes related to their employment.

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

The Superintendent or designee shall establish an Acceptable Use Agreement which outlines employee obligations and responsibilities related to the use of district technology. Upon employment and whenever significant changes are made to the district's Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

Employees shall not use district technology to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 6777; 47 USC 254)

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any equipment or other technological resources provided by or maintained by the district, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. To ensure proper use, the Superintendent or designee may monitor employee usage of district technology at any time without advance notice or consent and for any reason allowed by law.

In addition, employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct district business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of district technology to the Superintendent or designee.

Inappropriate use of district technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

Delano Union School District

Exhibit

Employee Use Of Technology

E 4040
Personnel

ACCEPTABLE USE AGREEMENT AND RELEASE OF DISTRICT FROM LIABILITY (EMPLOYEES)

The Delano Union School District authorizes district employees to use technology owned or otherwise provided by the district as necessary to fulfill the requirements of their position. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.

The district expects all employees to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable restrictions on the sites, material, and/or information that employees may access through the system.

The district makes no guarantee that the functions or services provided by or through the district will be without defect. In addition, the district is not responsible for financial obligations arising from unauthorized use of the system.

Each employee who is authorized to use district technology shall sign this Acceptable Use Agreement as an indication that he/she has read and understands the agreement.

Definitions

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Employee Obligations and Responsibilities

Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes. Any incidental personal use of district technology shall not interfere with district business and operations, the work and productivity of any district employee, or the safety and security of district technology. The district is not responsible for any loss or damage incurred by an employee as a result of his/her personal use of district technology.

The employee in whose name district technology is issued is responsible for its proper use at all times. Employees shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.

Employees are prohibited from using district technology for improper purposes, including, but not limited to, use of district technology to:

1. Access, post, display, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive

2. Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from a supervisor

3. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee

4. Engage in unlawful use of district technology for political lobbying

5. Infringe on copyright, license, trademark, patent, or other intellectual property rights

6. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission, changing settings on shared computers)

7. Install unauthorized software

8. Engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or district practice

Privacy

Since the use of district technology is intended for use in conducting district business, no employee should have any expectation of privacy in any use of district technology.

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to the Internet or social media, communications sent or received from district technology, or other uses within the jurisdiction of the district. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of district technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If an employee uses a personally owned device to access district technology or conduct district business, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

Records

Any electronically stored information generated or received by an employee which constitutes a district or student record shall be classified, retained, and destroyed in accordance with BP/AR 3580 - District Records, BP/AR 5125 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.

Reporting

If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of district technology, he/she shall immediately report such information to the Superintendent or designee.

Consequences for Violation

Violations of the law, Board policy, or this Acceptable Use Agreement may result in revocation of an employee's access to district technology and/or discipline, up to and including termination. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

Employee Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable Use Agreement, BP 4040 - Employee Use of Technology, and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology or when my personal electronic devices use district technology. I further understand that any violation may result in revocation of user privileges, disciplinary action, and/or appropriate legal action.

I hereby release the district and its personnel from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

Name: ______________________________ Position: ______________________
(Please print)

School/Work Site: ____

Signature: ______________________________ Date: ____________________