ACCEPTABLE USE AGREEMENT – EMPLOYEE/VOLUNTEER

The Burbank Unified School District authorizes district employees/volunteers 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/volunteers 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/volunteers 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/volunteer 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/Volunteer Obligations and Responsibilities

Employees/volunteers 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/volunteer, or the safety and security of district technology. The district is not responsible for any loss or damage incurred by employees/volunteers as a result of their personal use of district technology.

The employee/volunteer in whose name district technology is issued is responsible for its proper use at all times. Employees/volunteers 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/volunteers 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/volunteers shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.

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

1. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or unlawful discrimination, including discriminatory harassment, intimidation, and bullying, targeted at any employee or student by anyone, based on the employee or student's actual or perceived race, color, ancestry, nationality, national origin, immigration status, ethnic group identification, ethnicity, age, religion, marital status, pregnancy, parental status, physical or mental disability, sex, sexual orientation, gender, gender identity, gender expression, or genetic information, or association with a person or group with one or more of these actual or perceived characteristics. This includes political beliefs.

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 employees/volunteers 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/volunteers 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/volunteer on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If an employee/volunteer 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.

The following guidelines shall be followed when using personally owned devices to access BUSD resources:

1. Confidential information shall not be stored on mobile devices.

2. Keep mobile device operating systems and applications up-to-date with the latest security patches and enable automatic updates.

3. Secure all mobile devices with a strong password and encryption when possible.

4. Install and maintain appropriate endpoint security protection on mobile devices.

5. Report any suspected incident of unauthorized data access immediately to the Director of IT and Education Support.

6. Refrain from forwarding sensitive BUSD information to personal email accounts or to non-BUSD employees.

7. Refrain from leaving mobile devices unattended.

8. Refrain from using mobile devices to text or email while driving.

9. Agree and acknowledge that BUSD will establish audit trails to monitor access to internal BUSD resources and to identify unusual usage patterns or other suspicious activity. Audit trails may be accessed, published, and used without notice.

10. Participate in required training.

Records

Any electronically stored information generated or received by an employee/volunteer 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/volunteer 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/volunteer'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/Volunteer Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable Use Agreement, BP/AR 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.

_____ _____

Personnel Name:_____ Position: _____
(Please print)

School/WorkSite: _____

Employee / Volunteer (Please Circle)

Signature:_____ Date:_____