

Davis Joint Unified School District  
2018-2019 Student Acceptable Use of Technology Agreement

The Davis Joint Unified School District authorizes students to use technology owned or otherwise provided by the district as necessary for instructional purposes. 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 students 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 students may access through the system.

Each student who is authorized to use district technology and his/her parent/guardian shall sign this Acceptable Use Agreement as an indication that they have read and understand 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.

#### 21st Century Learner

Technology is an integral part of our students' lives and futures, and we strive to provide technology rich learning environment for students. Students need to learn and master the technology skills necessary to succeed in the technological 21st century global society. However, inappropriate use of these resources may result in disciplinary action and/or referral to legal authorities. The site administrator, district administrator, and/or systems administrator may limit, suspend, or revoke access to technology if deemed necessary.

#### Student Obligations and Responsibilities

Students are expected to use district technology safely, responsibly, and for educational purposes only. The student to whose name district technology is issued is responsible for its proper use at all times. Students 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.

Students 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, libelous, defamatory, obscene, sexually explicit, or disruptive
2. Bully, harass, intimidate, or threaten other students, staff, or other individuals ("cyberbullying")
3. Disclose, use, or disseminate personal identification information (such as name, address, telephone number, Social Security number, or other personal information) of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person
4. Infringe on copyright, license, trademark, patent, or other intellectual property rights
5. 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 from a teacher or other district personnel, changing settings on shared computers)
6. Install unauthorized software
7. "Hack" into the system to manipulate data of the district or other users
8. Engage in or promote any practice that is unethical or violates any law or Board policy, administrative regulation, or district practice

#### Filtering and Monitoring

As required by the Federal Children's Internet Protection Act (CIPA), content filtering technology is used to restrict access to unacceptable materials on all Internet access provided by DJUSD. The district makes every effort to limit access to objectionable material; however, no web filtering is 100% safe. With internet access a risk exists that students may access material that may not be of educational value in the school setting. Students who intentionally access, publish, or attempt to access or publish inappropriate or illegal material or Internet sites, may be subject to discipline; which may include the possibility of suspension or expulsion. If a student identifies a security problem, they are required to notify a teacher or administrator at once, and not demonstrate the problem to other users. Students should also never use another individual's account. All use of the system must be under your own account. If a user is identified as a security risk, he or she may be denied access to the information system and face potential disciplinary consequences.

#### Privacy

Since the use of district technology is intended for educational purposes, students shall not 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. 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. Students should be aware that, in most instances, their use of district technology (such as web searches and 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 a student on district technology does not create a reasonable expectation of privacy.

### Consequences for Violation

Violations of the law, Board policy, or this agreement may result in revocation of a student's access to district technology and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

### Student Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable Use Agreement 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. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

### Disclaimer of Liability

The District makes no guarantees about the quality of services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from the use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. The District denies any responsibility for material encountered on a computer network, including the Internet, which may be deemed objectionable to a user (or his/her parents, if a minor) or for any hostile or injurious actions of third parties encountered through a computer network. Any statement accessible on the computer network or the Internet is understood to be the author's individual point of view and not that of the District, its affiliates or employees. Due to the nature of electronic communications and changes in the law, it is also impossible for the District to guarantee confidentiality of email sent and received over any computer network. This Acceptable Use of Technology Agreement is consistent with the District's Board Policy and Administrative Regulation 6163.4. By signing an acknowledgment in Online Re-Enrollment, I affirm that I have read, understand, shared with my student and acknowledge receipt of this Acceptable Use Agreement.

Davis Joint Unified School District  
2018-2019 Employee Acceptable Use of Technology Agreement

The Davis Joint Unified 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, and District-approved social media.

#### 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,

May 23, 2018

Page 2 of 4

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. In the event of a lost or stolen district device, 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.

May 23, 2018

Page 4 of 4

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: \_\_\_\_\_