SAN BERNARDINO CITY UNIFIED SCHOOL DISTRICT
Employee Technology Responsible Use Agreement

The San Bernardino City Unified School District (SBCUSD) is providing employees access to the District's electronic network. This network includes Internet access, computer services, videoconferencing, computer equipment, mobile devices, and related equipment for District business. This document (hereinafter referred to as, "Agreement") contains the rules and procedures for employees' responsible use of the SBCUSD electronic network. This Agreement applies to all employees accessing the SBCUSD electronic network, all resources made available through the network, and all devices (District or personal) connected to the network. Employees should be advised that any personal devices – cell phones, tablets, laptops or personal computers – used by employees to conduct District business, may be subject to subpoena under the Public Records Act (G.C. 6250).

General Policies

- The SBCUSD electronic network has been established for specific educational purposes and for District business. The term "educational purpose" includes, but is not limited to, classroom activities, career development, and high-quality self-discovery activities.
- The SBCUSD electronic network has been established for educational purposes and not as a public access service or a public forum. San Bernardino City Unified School District has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- Employees must sign and adhere to this Agreement. The District is not responsible for the actions of employees who violate this Agreement. Access is a privilege — not a right.
- The District reserves the right to monitor all activity on the SBCUSD electronic network. Employees have no expectation of privacy with respect to usage of the electronic network, even if the use is for personal purposes. Any information or activity that is to be kept private must be accessed through personal accounts on personal devices.
- Employees may be held responsible for any damage that is caused by their inappropriate use of the network or equipment.
- Employees are expected to exercise sound judgment and professional demeanor, consistent with expectations for District employees and in compliance with law in the use of the SBCUSD electronic network.
- All personnel are expected to enforce all aspects of the Student Use of Technology Policy (BP 6163.4), Student Use of Technology Administrative Regulation (AR 6163.4), and Student Technology Responsible Use Agreement, as applicable, and to provide sufficient training and supervision of students to ensure students' compliance with the same.

Digital Citizenship Expectations

While utilizing any portion of the SBCUSD electronic network, employees are expected to exhibit responsible behavior and to refrain from engaging in inappropriate use. The SBCUSD electronic network is considered a limited forum, and therefore the District may restrict an employee's use of the network for valid reasons, including but not limited to, violations of the following:

- Employees shall not post information that, if acted upon, could cause damage or danger of disruption to the work and/or educational environment for staff and/or students.
- Employees shall not engage in electronic personal attacks, including prejudicial or discriminatory attacks that are in violation of any District policy, or State or Federal law.
- Employees shall act in accordance with the District's Non Discrimination Harassment Policy and shall not harass another person. If an employee is told by a person to stop sending messages, he/she must stop.
- Employees shall not knowingly or recklessly post false or defamatory information about a person or organization.
- Employees shall not use criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Employees shall not use speech that is inappropriate in an educational setting or violates District rules.
- Employees shall not abuse network resources such as sending chain letters or "spamming".
- Employees shall not display, access, or send offensive or pornographic/sexually explicit messages, pictures, or videos.
- Employees shall not use the SBCUSD electronic network for commercial purposes.
- Employees shall not use the SBCUSD electronic network for political lobbying.
- Employees shall not introduce and use any unauthorized wireless access points, routers, or switches in conjunction with the SBCUSD electronic network.
- Employees shall not use District equipment, the SBCUSD electronic network, or credentials to threaten employees, or to cause a disruption to the educational program or business environment.
- Employees shall not use District equipment, the SBCUSD electronic network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

- Employees shall not attempt to gain unauthorized access to District systems, (e.g., student information systems or business systems) without prior approval by their immediate supervisor and the District Information Technology/Accountability and Educational Technology Departments.
- Employees shall not utilize information obtained from student and/or business systems for unrelated business or personal purposes (i.e., the information will not be released to unauthorized persons and/or organizations and/or shared for personal reasons or personal gain including higher education research projects).

Electronic Communication

- All employees shall be provided with District email accounts for District business purposes.
- Employees may be provided with accounts that allow for messaging, chat, social networking, etc. These accounts are to be used for specific educational purposes or activities in accordance with State and Federal law.
- Employees shall not send or post private and/or personal information about another person without his/her permission.

Real-time, Interactive Communication Areas and Social Media

- Employees may use chat, instant messaging, and/or social media only for specific District business activities.
- When using social media resources (e.g., YouTube, social networking platforms, threaded discussion groups, blogs, etc.) for educational purposes, employees are expected to comply with all aspects of the Student Use of Technology Policy (BP 6163.4), Student Use of Technology Administrative Regulation (AR 6163.4), this Agreement, and the Student Technology Responsible Use Agreement.

Websites

- The use of any photographs or student work must follow District guidelines established by the Communications Department.
- Materials (graphics, text, sound, etc.) placed on any webpages are expected to meet academic standards of proper spelling, grammar, mechanics, and accuracy of information, and legal standards of copyright.
- All webpages must have a link back to the homepage of the classroom, school or District, as appropriate.

Message Board/Usenet Groups

- The District may provide access to selected newsgroups that relate to subjects appropriate for educational use. Messages posted locally that are in violation of this Agreement will be removed.

Telnet, File Transfer Protocol (FTP), and Remote Desktop Protocol (RDP)

- Telnet, FTP, and RDP services may be available to some employees. However, all aspects of this Agreement are applicable to material accessed or downloaded.

Personal Safety

- Employees shall not share personal contact and/or identifier information about other employees or students without appropriate authorization. Personal contact/identifier information includes, but is not limited to, address, telephone, school/work address, email address, Social Security Number, or employee ID number.
- Employees shall promptly disclose to a supervisor any electronic message received that is inappropriate or makes the employee feel uncomfortable.

System Security

- Employees are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them.
- Employees shall immediately notify a supervisor or the system administrator if they have identified a possible security problem. Employees should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Employees shall not attempt to gain unauthorized access to any portion of the SBCUSD electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Employees shall not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Employees shall not intentionally attempt to access websites blocked by District policy, including the use of proxy services, software, or websites.
- Employees shall not use sniffing or remote access technology to monitor the SBCUSD electronic network or other user's activity without authorization, or for malicious or unethical purposes.

Software and Files

- Software is available to employees to be used as an educational or business resource. Employees shall execute sound judgment in downloading and installing educational/ business software. Any software that causes disruption to the SBCUSD electronic network will be removed.
- Files stored on the SBCUSD electronic network are treated in the same manner as other business records. Routine maintenance and monitoring of the network by authorized employees may lead to discovery that an employee has violated

this Agreement or the law. Employees should not expect that files stored on District servers or accessed through the SBCUSD electronic network are private.

Technology Hardware

- Hardware and peripherals are provided as tools for employee use for educational and business purposes. Employees are not permitted to install or relocate network hardware and/or peripherals (except for portable devices), or to modify settings to equipment without the consent of the District Information Technology Department.

Vandalism

- Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software may result in suspension or cancellation of network privileges. Appropriate disciplinary action will be taken.

Plagiarism and Copyright Infringement

- Employees may access copyrighted material for instructional and/or business purposes.
- All employees are expected to follow existing copyright laws. Posting any material (graphics, text, sound, etc.) that is in violation of any federal or state law is prohibited. This includes, but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.
- Copyrighted material shall not be placed on any system without the author's permission. Permission may be specified in the document, on the system, or must be obtained directly from the author.
- Employees shall not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original work.

Videoconferencing/Classroom Video Feed

- All videoconferencing must be for District business and/or instructional purposes.
- Teachers and administrators shall not permit live feed and/or video recording of classroom instruction without proper authorization and in compliance with student privacy laws.
- Asynchronous presentations of classroom instruction are encouraged to provide expanded student access to instruction. These presentations can be posted to District approved sites (e.g., Learning Management System, website, and social media).

Due Process

- The District's authorized representatives will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the SBCUSD electronic network.
- Disciplinary actions will be tailored to meet specific concerns related to the violation. Violations of this Agreement may result in a loss of access as well as other disciplinary and/or legal action.

Limitation of Liability

- The District makes no guarantee that the functions or the services provided by or through the SBCUSD electronic network will be error-free or without defect. The District will not be responsible for any damage suffered, including but not limited to, loss of data, damage to personal devices, or interruptions of service.
- The District is not responsible for the accuracy or quality of the information obtained through or stored on the SBCUSD electronic network. The District will not be responsible for financial obligations arising through the unauthorized use of the network.

Violations of This Agreement

Violations of this Agreement may result in loss of access as well as other disciplinary and/or legal action. Employees' violation of this Agreement shall be subject to the consequences as indicated within this Agreement as well as appropriate disciplinary action(s), including but not limited to:

- Use of the SBCUSD electronic network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Appropriate District disciplinary action up to and including dismissal
- Legal action and prosecution by the authorities

The particular consequences for violations of this Agreement shall be determined by authorized District personnel. The Superintendent or designee and/or the Board shall determine when disciplinary action and/or legal action or actions by the authorities are the appropriate course of action.

SAN BERNARDINO CITY UNIFIED SCHOOL DISTRICT
Employee Technology Responsible Use Agreement Consent Form

Employee Name: _____

Job Title: _____ **School/Location**: _____

I understand I may be given access to components of the SBCUSD electronic network—which includes Internet access, computer services, videoconferencing, computer equipment and related equipment—for educational and business purposes.

I have read and understand the San Bernardino City Unified School District Employee Technology Responsible Use Agreement.

I agree to follow the terms contained in this Agreement.

Employee Signature: _____ **Date**: _____