Appendix A: CALPADS Rules of Behavior Agreement for CALPADS Local Users

I, as a CALPADS Local User, am acknowledging the following information:

1. I know and follow the security and privacy policies at my local education agency that are in place to protect the CALPADS data.
2. I know and follow the security and privacy state and federal laws that are in place to protect the CALPADS data.
3. I have a legitimate and authorized business need to access the data in CALPADS and will use this access only for legitimate and authorized business needs.
4. If I suspect or detect a security or privacy violation, I will contact the CALPADS Service Desk immediately as well as inform my local education agency in accordance with our policies.
5. If I am assigned one of the following roles: Direct Certification, Foster Youth, Free or Reduced Price Meals, and Special Education data, which is considered highly sensitive data, I will ensure that this data is handled with utmost privacy and security and every caution will be used in protecting this information from unauthorized access, exposure or distribution.
6. I have read, understand, and will comply with the following notice on the log in screen for CALPADS: "**NOTICE** -You are about to access the CALPADS computer system of the State of California Department of Education ("the Department"). This system is intended for authorized users only, in accordance with the Rules of Behavior Agreements for CALPADS Local Users, CALPADS LEA Administrators, and State Users, and applicable state and federal laws. Unauthorized access to or use of this system, or any information therein, is strictly prohibited by Department policy, the Rules of Behavior Agreements for CALPADS Local Users, CALPADS LEA Administrators, and State Users, and applicable state and federal laws. Unauthorized access to this system, and/or unauthorized use of information from this system may result in civil and/or criminal penalties under applicable state and federal laws. By using this system, you are acknowledging and agreeing that all information concerning your access to this system, including but not limited to any information entered, stored or retrieved by you, may be monitored, retrieved, and/or disclosed by authorized personnel, including authorized network administrators and CDE personnel, for any lawful purpose, including but not limited to criminal prosecution."
7. I understand that I am responsible for the security and privacy of my password. I will adhere to the following minimum requirements for a password: It must be at least eight (8) characters in length and must include at least one uppercase letter, at least one lowercase letter, and at least one of the following non-alphanumeric characters: ! ? @ # $ ^ & * -= _ +.
8. I will comply with the following rules governing user credentials: I will protect my logon credentials at all times, never share my user ID and/or password with anyone, avoid using a feature in my local browser which automatically fills in passwords, and avoid writing my password down. (If I need to write my password down, I will keep this information in a secure area.)

9. I will protect CALPADS information in any form, including information contained on printed reports, data downloaded onto computers and computer media (e.g., diskettes, tapes, compact discs, thumb drives, etc.), user computer monitors, or any other format. Data which is saved to portable storage devices, such as laptops, USB thumb drives, DVD's, and discs will be encrypted.

10. I will log out of CALPADS if I am going to be away from my computer, log out of CALPADS or lock my computer before I leave it unattended, remove CALPADS media information from my desktop when I am away from my desk, store media containing CALPADS information in a locked container during non-business hours, properly cleanse or destroy media containing CALPADS information, and shred paper media and compact discs prior to disposal. I will cleanse diskettes and other magnetic media using appropriate software or a magnetic field with sufficient strength so as to make the information unreadable. I understand that simply deleting files from magnetic media does not remove the information from the media.

11. I am aware of the security issues of snooping, shoulder surfing, social engineering, faxing, virus scanning and patching, phishing, spear phishing breaches from these issues to the best of my ability.