# California Longitudinal Pupil Achievement Data System (CALPADS)

## CALPADS LEA ADMINISTRATOR APPLICATION AND GUIDELINES

***Version 9.2***

***September 19, 2018***

**California Department of Education**

# Table of Contents

**Revision History**

| Version Number | Revision Date | Name | Section | Summary of Changes |
|---|---|---|---|---|
| v9.2 | 09/19/18 | CALPADS Operations Office | Appendix A & B, Application | Password requirements; security question. |
| v9.0 | 01/31/18 | CALPADS/CBEDS/ CDS Operations Office | All | Format changed and updated version number to correspond with other CALPADS documentation |
| v9.0 | 01/22/18 | CALPADS/CBEDS/ CDS Operations Office | All | Updated privacy and security requirements |
| v3.0 | 07/01/16 | CALPADS/CBEDS/ CDS Operations Office | All | Updated privacy and security requirements |
| v2.4 | 01/29/15 | CALPADS/CBEDS/ CDS Operations Office | Sections A, C, E and Application | Updated application submission instructions and signature block |
| v2.3 | 06/19/12 | CALPADS Operations Office | State & Federal Privacy Laws | Updated Web page URL |
| v2.2 | 09/16/11 | CALPADS Operations Office | All | Field for Internal Use |
| v2.1 | 08/22/11 | CALPADS Operations Office | All | Converted to fillable form |
| v2.0 | 01/03/11 | CALPADS Operations Office | All | Updated CALPADS Service Desk contact information |
| v1.0 | 07/10/09 | CALPADS Operations Office | All | Initial draft release |

# CALPADS LEA Administrator Application Overview

## Introduction

Each local educational agency (LEA) must have at least one, but no more than two, California Longitudinal Pupil Achievement Data System (CALPADS) LEA Administrator(s) designated by the Superintendent or independently reporting Charter (IRC) School Administrator. The CALPADS LEA Administrator receives authorization to access CALPADS from the California Department of Education (CDE). Upon receiving access rights to CALPADS, the CALPADS LEA Administrator is authorized to grant access rights to their Local Users, at different levels and for specific roles, depending upon the users' legitimate business needs. CALPADS LEA Administrators are responsible for overseeing the use of CALPADS by their Local Users. LEAs can retain access to CALPADS at the district level or provide access to local sites (including charter schools). For example, some LEAs may decide to centralize the acquisition and maintenance of Statewide Student Identifiers (SSIDs) at the district level, while other LEAs may decide to delegate this

activity to each school. In all instances, LEAs must have security and privacy policies in place to protect the personally identifiable data in CALPADS.

## Purpose of Document

The purpose of this document is to outline the application procedure the CDE uses to grant CALPADS LEA Administrators access to CALPADS.

## CDE Contact Information

If you have any questions, please contact the CALPADS Service Desk by visiting the FCMAT/CSIS CALPADS Web page at http://csis.fcmat.org/Pages/CALPADS.aspx (in the "Quick Links" box on the upper right hand side of page under the "Support Resources" heading, click on "CALPADS Online Support Form"), via e-mail at calpads-support@cde.ca.gov, or by Phone at 916-325-9210.

## CALPADS Roles

The following are roles and responsibilities for CALPADS access:

**The CDE CALPADS LEA Administrator**: The CDE staff responsible for providing initial approval and confirming the final approval of the CALPADS LEA Administrator application, and creating CALPADS LEA Administrator accounts.

**Superintendent or independently reporting Charter (IRC) School Administrator:** The individual responsible for verifying the identity of an applicant for the CALPADS LEA Administrator role, attesting to the applicant's qualifications for the CALPADS LEA Administrator role, and confirming that the applicant's data privacy training is appropriate to secure the data access provided by the state for this role, including access to Direct Certification, Foster Youth, Free or Reduced Price Meals, and Special Education data, which are considered highly sensitive data.

The Superintendent or IRC School Administrator is responsible for ensuring that these data are handled with utmost privacy and security and that every caution is used in protecting this information from unauthorized access, exposure or distribution. Specifically, the Superintendent or IRC School Administrator is responsible for:

- Verifying the identity and qualifications of the CALPADS LEA Administrator on an annual basis as part of the CALPADS LEA Administrator application.
- Ensuring the integrity of the CALPADS LEA Administrator application process by preventing unauthorized users from applying for administrative access rights.
- Confirming the CALPADS LEA Administrator completes mandatory annual privacy and security training provided by the California School Information Services (CSIS).
- Having policies and procedures in place for notifying CDE when there are any changes in personnel or job duties which impact the CALPADS LEA Administrator assignment. This includes notifying the CALPADS Service Desk immediately when there is a change in one or both of the CALPADS LEA Administrators so that the CDE can de-activate CALPADS LEA Administrator accounts.
- Having policies and procedures in place for ensuring the transition of responsibilities when there is a change in Superintendent or Charter School Administrator. A new CALPADS LEA Administrator application with a new signature is due to the CDE within 30 days of the new Superintendent or Charter School Administrator taking office.
- Ensuring the CALPADS LEA Administrator and all local users of CALPADS abide by the agreements set forth in Appendix A and Appendix B of this document.
- Contacting the CALPADS Service Desk immediately following a known or suspected breach or unauthorized use of CALPADS.

- Ensuring the accuracy of data submitted and certified in CALPADS as part of the Fall and End-of-Year submissions by the deadlines.

If the LEA uses a third party vendor as an administrator for CALPADS, the Superintendent or IRC School Administrator must ensure that the vendor(s) is under the LEA's direct control and that the LEA has a contract with the third party vendor that meets all of the requirements set forth in Education Code section 49073.1 in order to protect student data privacy.

**CALPADS LEA Administrator:** LEAs must submit an application signed by the Superintendent or Charter School Administrator and receive approval by the CDE of the CALPADS LEA Administrator on an annual basis. LEAs may have up to two CALPADS LEA Administrators.

The CALPADS LEA Administrator is provided the CALPADS LEA Administrator Role which enables the CALPADS LEA Administrator to create accounts and grant roles to local district and school users. The CALPADS LEA Administrator must abide by the agreement set forth in Appendix B and is responsible for ensuring Local Users abide by the agreements set forth in Appendix A.

**Local User:** Local Users are individuals who have been provided access to CALPADS by the CALPADS LEA Administrator. Local Users are given accounts and may be provided different local roles as granted by the CALPADS LEA Administrator based on business need. Local Users must abide by the agreement set forth in Appendix A.

It is the responsibility of any CALPADS user to protect the confidentiality of information stored in the system. CALPADS users that are issued a CALPADS account must be currently employed by the school, district, or county office or contracted by the LEA, and must have a legitimate business need to input, modify, or view data in CALPADS. When determining roles and qualifications for Local User access to CALPADS, it is imperative that the CALPADS LEA Administrator align the legitimate business needs of the potential user with the functionality and purpose of the CALPADS system.

## CALPADS Accounts

**LEA Account:** The CALPADS LEA Administrator can provide Local Users an LEA Account to perform the following:

- Map local codes to CALPADS codes;
- Review county and authorizing LEA reports;
- Certify data for Fall 1, Fall 2, End of Year (EOY) 1, EOY 2, and EOY 3;
- Perform any other function that is available under a School Account (see below) that is assigned by the CALPADS LEA Administrator to the Local User.

All CALPADS LEA Administrators are provided an LEA account and are granted the CALPADS LEA Administrator role by the CDE. CALPADS LEA Administrators must provide Superintendents or Charter School Administrators an LEA Account to certify data.

**School Account:** CALPADS LEA Administrator can provide School Accounts to Local Users to perform specific functions (e.g. upload/update data, view reports) for students enrolled at the school. The School Account cannot be used for mapping local codes, reviewing county and authorizing LEA reports, and certifying data. Appendix A describes the responsibilities of Local Users with School Accounts and what the user must agree to before accessing CALPADS. The CALPADS LEA Administrator is responsible for the security of data exposed through this account.

## User Account Creation

In the dropdown from the Help tab in CALPADS, instructions and procedures are provided in the *LEA Operations Manual* that the CALPADS LEA Administrator must utilize when authorizing access rights to Local Users.

## State and Federal Privacy Laws

In order to comply with federal and state privacy law and regulations, CALPADS is to be used by only authorized users and only for legitimate business needs.

All CALPADS LEA Administrators, Superintendents or IRC School Administrators should review and become familiar with state and federal privacy laws, located on the State of California Department of Justice Office of the Attorney General's Privacy Enforcement & Protection Unit Web page at https://www.oag.ca.gov/privacy/privacy-enforcement-laws-legislation. This should be reviewed on an annual basis as laws are continually changing.

The CDE has additional resources available at http://www.cde.ca.gov/ds/dp/. It is ultimately the responsibility of each LEA to access and use the data in CALPADS in compliance with all legal requirements.

## Incident Response Requirement

If any CALPADS user suspects or detects a security or privacy violation, the CALPADS Service Desk should be contacted immediately. For example, if you suspect someone may have used your user ID to log on to CALPADS, you should contact the CALPADS Service Desk. Other warning signs that CALPADS may have been compromised include, but are not limited to:

- inappropriate images or text on the Web pages;
- data formats that are not what is expected;
- missing data; or
- CALPADS is not available.

While these may not be attributed to a compromise, it is better to have it checked out and be sure than to take no action.

# CALPADS User Responsibilities and Rules of Behavior Agreements Specific to the CALPADS LEA Administrator or Local Users

## Introduction

The CDE requires all CALPADS users to review and consent to the appropriate Rules of Behavior Agreement before receiving access to CALPADS. It is the responsibility of the CALPADS LEA Administrator to confirm that the Rules of Behavior Agreement is reviewed and understood by each Local User given access to CALPADS by the CALPADS LEA Administrator. The CALPADS LEA Administrator must review and understand the Rules of Behavior Agreement for the CALPADS LEA Administrator role as well as all of the information in this entire document. The Rules of Behavior Agreement contains important information concerning system security and provides examples of behaviors that are recommended to protect the privacy and confidentiality of CALPADS information. We appreciate your cooperation with reviewing all materials prior to accessing the system. The Rules of Behavior Agreements for the CALPADS Local Users and LEA Administrator are in Appendix A and B, respectively, of this application.

## Banner Agreement Upon Log On

All LEA representatives that are authorized to access CALPADS will see the following banner language upon each log on:

"**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 CALPADS Rules of Behavior Agreement, 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 CALPADS Rules of Behavior Agreement, 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 personnel, including network administrators and CDE personnel, for any lawful purpose, including but not limited to criminal prosecution."

## System Security

CALPADS is a CDE information system to be used for official use only. The topics addressed in this document provide security information specific to the CALPADS system. It is important that you read through the entire text. All CALPADS users are required to agree to the CALPADS Rules of Behavior Agreement specific to their user role in order to understand the privacy and security requirements related to use of CALPADS.

## CALPADS Security Controls

CALPADS roles are a part of the security controls implemented to protect the information processed and stored within the system. When CALPADS LEA Administrators provide access to CALPADS, the CALPADS LEA Administrator is responsible to ensure that the access to CALPADS is limited to the required business need of the Local User. CALPADS users are an integral part in ensuring the CALPADS security controls provide the intended level of protection. Specifically, these control settings are designed to:

- Protect the privacy and confidentiality of the system information;
- Ensure only authorized users access the system;
- Ensure users are uniquely identified when using the system;
- Connect actions taken within the system to a specific user;
- Ensure users only have access to perform the actions required by their position;
- Ensure CALPADS information is not inappropriately released; and
- Ensure CALPADS is available to authorized users when needed.

## User Credentials

User credentials include a user ID and password, and are the control mechanism by which CALPADS identifies and verifies users. .

User ID uniquely identify individual CALPADS users and allow the CDE to enforce system accountability by assigning specified roles to individual users. CALPADS LEA Administrator user IDs will be created by CDE. More information is provided in the *LEA Operations Manual* accessible from within CALPADS.

CALPADS creates the user's initial, temporary, password that must be changed to continue using the system. Passwords must:

- Be at least eight characters and up to fifteen characters in length
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Contain at least one of the following non-alphanumeric characters: ! @ # $ ^ & * - = _ + ?

Password must **not** be:

- Same as the user ID
- Same as the current password
- Posted in a public place or on a sticky, attached to your monitor

Passwords expire every 90 days and must be renewed. You will be prompted when a new password is needed.

A strong password consists of at least 10 characters and includes a combination of uppercase and lowercase letters, numbers, and symbols. A unique password is a password that is only used with one account

It is important for you to comply with the following rules governing user credentials:

- Protect your user credentials at all times;
- Never share your user ID and/or password with anyone;
- Avoid writing your password down (however, if you need to write your password down, please keep it in a secure area); and
- Avoid using the “remember password” feature in your local browser.

## Protection of CALPADS Information

You are required to protect CALPADS information in any form. This includes 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 must be encrypted.

In order to ensure protection of CALPADS information, users should follow these guidelines:

- Log out of CALPADS if you are going to be away from your computer.
- Log out of CALPADS or lock your computer before you leave it unattended (e.g., use the < Ctrl > < Alt > < Delete > key sequence when leaving your PC workstation).
- Media (including reports) containing CALPADS information should be removed from your desktops when you are away from your desk.
- Store media containing CALPADS information in a locked container during non-business hours (e.g. desk drawer).
- Media containing CALPADS information should be properly wiped or destroyed:
  - Shred paper media and compact discs prior to disposal.

    - Diskettes and other magnetic media should be cleansed using appropriate software or a magnetic field with sufficient strength so as to make the information unreadable.
    - Note that simply deleting files from magnetic media does not remove the information from the media.
- Media containing encrypted information can be excluded from the cleansing process, although cleansing all media is recommended.
- CALPADS LEA Administrators should grant only the appropriate access level required by Local Users to fulfill their job duties. Do not disclose CALPADS information to any individual without a "need-to-know" for the information in the course of their business.

### Other Security Issues

This section describes some additional security items of which you should be aware:

- **Snooping**: Snooping is when a user has legitimate access to a system but accesses data outside of the course of performing his/her job duties. Snooping is prohibited. For example, you may be responsible for entering and updating Statewide Student Identifiers (SSID's) but have access to assessment records. Snooping occurs if you view assessment records for a particular student and obtain information that is not relevant to your assigned job responsibilities. If you have access to more information than what is necessary to perform your job duties, please notify your CALPADS LEA Administrator to make the appropriate modifications to your user account.
- **Shoulder Surfing**: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. An example of shoulder surfing is when a person looks over someone else's shoulder while they are entering a password for a system to covertly acquire that password. To protect against this, be aware of your surroundings and prevent the accidental disclosure of information when entering your password or viewing information on your computer monitor.
- **Social Engineering**: Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. For example, a typical social engineering attack scenario is a hacker posing as an authorized user calling a system service desk posing as that user. The hacker, through trickery, coercion, or simply being nice coaxes the service desk technician into providing the login credentials for the user he is claiming to be. The hacker then gains unauthorized access to the system using an authorized user's credentials. To defeat social engineering, never provide credentials or confidential information.
- **Faxing**: When faxing CALPADS information, call the recipient of the fax and let them know it is coming. Ask them to go to the fax machine so they can pull it off right away so any sensitive information is not left lying around the office.
- **Virus Scanning and Patching**: Maintain current operating system patches and virus definitions to protect your computer. Scan documents or files downloaded to your computer from the Internet for viruses and other malicious code. Virus scanning software should also be used on e-mail attachments.

## Applicant Process & Instructions

The steps in Table 1 outline the complete application process for the CALPADS LEA Administrator to request access to CALPADS:

*Table 1 - Applicant Process & Instructions*

| Step | Action |
|---|---|
| 1 | The LEA submits a CALPADS Service Desk ticket requesting the CALPADS LEA Administrator Application and Guidelines |
| 2 | The applicant and the Superintendent or IRC School Administrator receives an electronic version of the CALPADS LEA Administrator Application and Guidelines from the CDE and reads the entire guidelines and application document. |
| 3 | The applicant completes Sections A and B, signs, and dates the application providing relevant applicant and account information including, but not limited to, a valid work e-mail address, work telephone number, LEA/School name and CD Code/CDS Code that will be used to create the account. |
| 4 | The applicant forwards the application to the Superintendent or IRC School Administrator for approval and signature. |
| 5 | The LEA scans the completed and signed application, and attaches the electronic version of the application to the original CALPADS service request email. If the original service request is not available, the LEA may attach the application to a new service request by going to the CALPADS Online Support form in "Support Resources" Quick Links at http://csis.fcmat.org/Pages/CALPADS.aspx. If the LEA is unable to submit the application via service request, they may submit it to the California Department of Education, CALPADS Operations Office by fax at 916-327-0195 or by mail at 1430 N Street, Suite 6416, Sacramento, CA 95814. |
| 6 | Applications are valid for one year. Therefore, LEAs should ensure that a new application is submitted to the CDE prior to the existing application's expiration. |

Please review the instructions below to understand what is required of the applicant to complete the application form. Asterisks (*) indicate required fields.

## A. REQUEST TYPE

1. **New Account** - Check this box if you are requesting a new CALPADS LEA Administrator account.
2. **Existing Account** - Check this box is you are requesting action for an existing CALPADS LEA Administrator account. Choose all of the following that apply:

   **Password Reset** - Request to reset your password
   **Yearly Renewal** - Submitting an application to replace an application that is more than one year old.
   **Update email** - Change the email address associated to your existing CALPADS LEA Administrator account.

## B. APPLICANT INFORMATION

3. **First Name*** - The first name of the individual requesting access to CALPADS (hereinafter "applicant").
4. **Last Name*** - The applicant's last or surname.
5. **Title* -** The applicant's job title or description.
6. **Work e-mail* -** The applicant's workplace e-mail address.
7. **Work Telephone*** - The applicant's workplace area code and telephone number**.**

8. **Work Address*** - The applicant's workplace street address.
9. **Work City*** – The applicant's workplace city.
10. **Work State*** – The applicant's workplace state.
11. **Work Zip*** – The applicant's workplace zip code.
12. **District or Independently Reporting Charter Name*** – The name of the district (includes single school districts) or (IRC) school for which the applicant is requesting CALPADS access.
13. **14 Digit County-District-School (CDS) Code or 7 Digit County-District (CD) Code*** – The 14 digit CDS code associated to the district or IRC school for which the applicant is requesting CALPADS access. If you are not requesting access to an IRC school, use your county office or district's 7 digit County-District (CD) code (e.g. 64-09876). For a list of current CDS codes, visit CDE's California School Directory Web page at http://www.cde.ca.gov/schooldirectory/
14. **Security Question* -** Check one box only to choose a security question (*these are not the same Security Questions the applicant sets up within CALPADS to reset their password*).
    - What is the name of your favorite teacher?
    - What is the name of your childhood best friend?
    - What was the first musical instrument that you learned to play?
15. **Answer*** - Enter the answer to the Security Question chosen in box 14. The answer will be used to verify the CALPADS LEA Administrator's identity via phone or through a CALPADS Service Desk request if they require a password reset or any other changes or updates to an existing CALPADS LEA Administrator account.
16. **Signature*** - The applicant's signature acknowledges that a hard copy of the signed application is on file in a secure location. A signature is required on the electronic application submitted to the CDE for processing.
17. **Date*** - The date the applicant signed the application.

## Submit to Superintendent or IRC School Administrators

The identity of the CALPADS LEA Administrator must be verified by the Superintendent or IRC School Administrator that serves within the official reporting structure as found on the California School Directory Web page at http://www.cde.ca.gov/re/sd/. Further, the Superintendent or IRC School Administrator must attest to the applicant's legitimate business need for access to CALPADS as an administrator and accept responsibility for the administrator's actions, including appropriate assignment of user roles.

The LEA may authorize up to two CALPADS LEA Administrators. In this case, an application must be completed by the primary CALPADS LEA Administrator and a second application must be completed by any secondary CALPADS LEA Administrator. The LEA must contact the CDE if more than one CALPADS LEA Administrator is required. CALPADS LEA Administrators are not authorized to create additional CALPADS LEA Administrator accounts. *(Note: If the CALPADS LEA Administrator is responsible for more than one LEA, then the Superintendent or IRC School Administrator from each LEA is accountable for the administrator, and must complete and sign a separate application form. In this case, the CALPADS LEA Administrator should forward a separate application to each respective Superintendent or IRC School Administrator for signatures*.)

A copy of all signed applications must be sent to the CDE.

## Superintendent or IRC School Administrator Process Instructions

The steps in Table 2 outline the complete application process for the Superintendent or IRC School Administrator to verify the CALPADS LEA Administrator application:

*Table 2 - Superintendent or IRC Administrator Process Instructions*

| Step | Action |
|---|---|
| 1 | The Superintendent or IRC School Administrator completes Section C of the application. This information must be consistent with the information provided on the California School Directory Web page at http://www.cde.ca.gov/re/sd/. |
| 2 | The Superintendent or IRC School Administrator reviews the entire application for completeness and accuracy. |
| 3 | The Superintendent or IRC School Administrator verifies the applicant's identification and current employment with the LEA. |
| 4 | The Superintendent or IRC School Administrator attests to the applicant's need for a CALPADS LEA Administrator role, and confirms the appropriate level of access has been authorized. |
| 5 | Upon completion, the Superintendent or IRC School Administrator signs the hard copy of the application and agrees to store the signed hard copy application in a secure location (e.g., locked file cabinet) for state audit purposes. A copy of the signed document is sent to the CDE. |

Please review the instructions in section C below to understand what is required of the Superintendent or IRC School Administrator to complete the application form.

## C. SUPERINTENDENT OR IRC SCHOOL ADMINISTRATOR IDENTIFICATION, VERIFICATION, ATTESTATION & SIGNATURE

18. **First Name*** - The superintendent or IRC school administrator's first name.
19. **Last Name*** - The superintendent or IRC school administrator's last or surname.
20. **Title* -** The superintendent or IRC school administrator's job title or description.
21. **Work e-mail* -** The superintendent or IRC school administrator's workplace e-mail address.
22. **Work Telephone*** - The superintendent or IRC school administrator's workplace area code and telephone number**.**
23. **Work Address*** - The superintendent or IRC school administrator's workplace street address.
24. **Work City*** – The superintendent or IRC school administrator's workplace city.
25. **Work State*** – The superintendent or IRC school administrator's workplace state.
26. **Work Zip*** – The superintendent or IRC school administrator's workplace Zip code.
27. **District or Independently Reporting Charter Name*** – The name of the district or IRC for which the superintendent or IRC school administrator is responsible.
28. **14 Digit County-District-School (CDS) Code or 7 Digit County-District (CD) Code *** – The 14 digit CDS code associated to the district or IRC school for which the applicant is requesting CALPADS access. If you are not requesting access to an IRC school, use your county office or

district's 7 digit County-District (CD) code (e.g. 64-09876). For a list of current CDS codes, visit CDE's California School Directory Web page at http://www.cde.ca.gov/schooldirectory/

29. **Superintendent or Independently Reporting Charter School Administrator Signature***: - The Superintendent's or IRC School Administrator's signature acknowledges that they have authenticated the applicant's identity (e.g., reviewing State/District issued ID badge, driver's license, passport, etc.), confirmed that the assigned role and level of access is consistent with the applicant's job duty, and that a hard copy of the signed application is on file in a secure location. A signature is required on the electronic application submitted to CDE for processing.
30. **Date***: The date the Superintendent or IRC School Administrator signed the application.

### Submit Application

After completing the electronic version of the application, reply to the original service request ticket and attach a completed, signed electronic version of the application. If the original service request is not available, go to CALPADS Online Support form in "Support Resources" Quick Links at http://csis.fcmat.org/Pages/CALPADS.aspx to submit the completed application via a new service request. If you are unable to submit the application via service request, you may submit it to the California Department of Education, CALPADS Operations Office by fax at 916-327-0195 or by mail at 1430 N Street, Suite 6416, Sacramento, CA 95814. It is the responsibility of the LEA to retain a hard copy of the application with valid signatures for school records and auditing purposes.

### Processing CALPADS LEA Administrator Changes

To enroll new or additional CALPADS LEA Administrators, submit an application as described above. To remove existing CALPADS LEA Administrators, submit a CALPADS Service Desk request by using the CALPADS Online Support form in "Support Resources" Quick Links at http://csis.fcmat.org/Pages/CALPADS.aspx or via phone at (916) 325-9210.

## CDE Approving Authority Process

The steps in Table 3 outline the approval process the CDE will use to authorize the creation of the CALPADS LEA Administrator user account:

*Table 3 - CDE Approving Authority Process*

| Step | Action |
|---|---|
| 1 | The CDE CALPADS LEA Administrator will review the application to verify that both the applicant and Superintendent or IRC School Administrator sections are complete and signed. The CDE CALPADS LEA Administrator will check that the name of the Superintendent or Charter School Administrator is the same as the Superintendent or Charter School Administrator on record in the California School Directory. If any problems emerge during the review, the CDE staff will contact the applicant and/or the Superintendent or IRC School Administrator to obtain additional information. |
| 2 | Upon successfully completing the review, the CDE staff will create an account for the applicant. |

## CDE Account Creation and Access

The steps in Table 4 outline the complete process the CDE will use to create the CALPADS LEA Administrator user account:

*Table 4 - CDE Account Creation and Access*

| Step | Action |
|---|---|
| 1 | Once the new user account application is complete with the appropriate signatures, the CALPADS Service Desk will send an e-mail notification of initial receipt. Once the user ID has been created and entered into CALPADS, the system will send an e-mail with the new user's temporary password. This will be followed by a confirmation e-mail from the CDE to the applicant with the new user's ID. |
| 2 | New users will be required to use the assigned CALPADS LEA Administrator user ID and temporary password to log on to CALPADS to reset their temporary password when first accessing CALPADS. |
| 3 | CALPADS LEA Administrators must contact the CALPADS Service Desk to make any changes to their Administrator account, such as changes to their name, work address, or e-mail address. |

# CALPADS LEA Administrator Application

*Attach a completed, signed and scanned electronic version of this application to your original CALPADS service request e-mail. If your original service request is not available, go to CALPADS Online Support form in "Support Resources" Quick Links at http://csis.fcmat.org/Pages/CALPADS.aspx to submit your completed application via a new service request. If you are unable to submit your application via service request, submit it to the California Department of Education, CALPADS Operations Office by fax at 916-327-0195 or by mail at 1430 N Street, Suite 6416, Sacramento, CA 95814. Asterisks (*) indicate required fields. Mouse over the field for instructions.*

| **A. REQUEST TYPE*** (*Choose 1. **or** 2.*) | |
|---|---|
| 1. ☐ New Account | 2. ☐ Existing Account *(choose all that apply)*<br>☐ Password Reset ☐ Yearly Renewal ☐ Update email<br>☐ Other *(explain)*_____ |

| **B. APPLICANT INFORMATION** | | | | |
|---|---|---|---|---|
| 3. First Name* | | 4. Last Name* | | |
| 5. Title* | 6. Work e-mail* | | 7. Work Telephone* | |
| 8. Work Address* | | 9. Work City* | 10. Work State* | 11. Work Zip* |
| 12. District or Independently Reporting Charter Name* | | 13. 14 Digit CDS Code or 7 Digit CD Code* | | |

| | | |
|---|---|---|
| 14. Security Question* *(choose only one)* | ☐ What was the name of your favorite teacher?<br>☐ What was the name of your childhood best friend?<br>☐ What was the first musical instrument that you learned to play? | 15. Answer* |

I certify by my signature on this form that this information is accurate and complete. I will only use CALPADS in accordance with the guidelines set forth in this application and will abide by the CALPADS Rules of Behavior specific to the CALPADS LEA Administrator, including ensuring that appropriate local security controls and processes are in place and that Local Users are monitored for compliance with data security and privacy requirements. I will attend and complete annual CALPADs trainings, and annually review data privacy and security laws and requirements for compliance. I will store this completed signed application, containing original signatures, in a secure location.

| 16. Applicant Signature* | 17. Date* |
|---|---|

| **C. SUPERINTENDENT OR INDEPENDENTLY REPORTING CHARTER SCHOOL ADMINISTRATOR IDENTIFICATION, VERIFICATION, ATTESTATION & SIGNATURE** | | | | |
|---|---|---|---|---|
| 18. First Name* | | 19. Last Name* | | |
| 20. Title* | 21. Work e-mail* | | 22. Work Telephone* | |
| 23. Work Address* | | 24. Work City* | 25. Work State* | 26. Work Zip* |
| 27. District or Independently Reporting Charter Name* | | 28. 14 Digit CDS Code or 7 Digit CD Code * | | |

I certify that: 1) I have verified the identity of the above CALPADS LEA Administrator applicant and determined that he or she is currently employed with the LEA stated above, has a legitimate business need for administrative access to CALPADS and is qualified for this role; 2) I am responsible for overseeing the CALPADS LEA Administrator and ensuring that CALPADS will only be used in accordance with the guidelines in this application and in compliance with all privacy and security laws; 3) the CALPADS LEA Administrator will complete mandatory annual CALPADS training; and 4) I will store this completed signed application, containing original signatures, in a secure location.

| 29. Superintendent or Independently Reporting Charter School Administrator Signature* | 30. Date* |
|---|---|

# 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. 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 characters from three of the four categories: at least one uppercase letter, at least one lowercase letter, at least one number, 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, and whaling, and I will prevent breaches from these issues to the best of my ability.

# Appendix B: Rules of Behavior Agreement for CALPADS LEA Administrators

By signing the CALPADS LEA Administrator Application, I, as a CALPADS LEA Administrator, agree to abide by the terms and conditions of usage and accept all ramifications of the policies and 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. I understand that this role has access to 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 characters from three of the four categories: at least one uppercase letter, at least one lowercase letter, at least one number, 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, and whaling, and I will prevent breaches from these issues to the best of my ability.
12. I will complete the annual CALPADS LEA Administrator application process and will attend and complete the annual CALPADS training on privacy and security.
13. I will configure available LEA system features to make certain that appropriate local security controls and processes are in place.
14. I will monitor Local Users for compliance with CALPADS data security and privacy requirements.
15. I will assign, maintain, and review Local User access privileges and accounts to ensure that only users with a required business need have access to CALPADS.
16. I will review the *LEA Operations Manual* in CALPADS and comply with all CALPADS requirements as a CALPADS LEA Administrator.
17. If the Superintendent or Charter School Administrator that signed my application is no longer in that position due to retirement, termination, death or any other reason, I will complete a new CALPADS LEA Administrator application with the signature of the new Superintendent or Charter School Administrator as required.