TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 NORTH LAMAR BOULEVARD
POST OFFICE BOX 4087, AUSTIN, TX 78773-0252
512/424-2365

SCHOOL CONTRACTOR DOCUMENT PACKET

This packet contains the documents required for school contractors to submit fingerprints of applicants for national criminal history reviews, as required under Senate Bill 9. The packet includes:

1. **Guide for School Contractors**
   Please follow these step-by-step directions
   The ORI for the DPS Secure Website referenced in these instructions is
   https://secure.txdps.state.tx.us/DPS_WEB/Portal/AccountManager/index.aspx
   Follow the instructions on this page to establish your account according to the guide for the School Contractors

2. **DPS Security Policy for Non-Criminal Justice Agencies**
   Read these security requirements carefully. You must follow them in accessing and using the criminal history data. The policy may change in the future and you will be required to any modifications.

3. **Contractor Entity Agreement for the Fingerprint-based Applicant Clearinghouse of Texas (FACT)**
   As stated in the Guide, please complete this agreement and return it to the Access and Dissemination Bureau.

4. **Authorized User Acknowledgement Agreement**
   Each employee of your company that uses the FACT Clearinghouse must sign this document and follow its requirements.

5. **Criminal Penalty for the Unauthorized Obtaining, Use, or Disclosure of Criminal History Information**

6. **Criteria for Approval to Access Criminal History Information**
   Criteria for approval to access criminal history information through the DPS databases.

Contact the Access and Dissemination Bureau with any questions.

Access and Dissemination Bureau
Texas Department of Public Safety
Crime Records Service
P. O. Box 149322
Austin, Texas 78714-9322

Email: FACT@txdps.state.tx.us
Phone: (512) 424-2365

DPS AND FBI CRIMINAL HISTORY CHECKS GUIDE FOR SCHOOL CONTRACTORS

Legislative Requirement

Senate Bill 9 passed in the most recent legislative session directs school district contractors to obtain state and national criminal history background searches on their employees who:

> *On or after January 1, 2008, is offered employment by an entity that contracts with a school district, open-enrollment charter school, or shared services arrangement to provide services, if:*
>
> *(1) the employee or applicant has or will have continuing duties related to the contracted services; and*
>
> *(2) the employee or applicant has or will have direct contact with students.*

The bill states that DPS will provide the results through the DPS criminal history clearinghouse (Fingerprint-based Applicant Clearinghouse of Texas –FACT). FACT is a new service developed by the DPS to fulfill the background check requirements of non-criminal justice entities. Initially FACT will serve the Texas Education Agency (TEA), school districts, charter schools, and school contractors as required by Senate Bill 9.

The Process

Briefly stated, school contractors must take the following steps to obtain the background checks required under Senate Bill 9:

1. **Establish an account on the DPS FACT clearinghouse, as follows:**

    a. Contact the DPS Access and Dissemination Bureau and advise them that you are applying for access as a school contractor:

    Access and Dissemination Bureau
    Texas Department of Public Safety
    Crime Records Service
    P. O. Box 149322
    Austin, Texas 78714-9322

    Email: FACT@txdps.state.tx.us
    Phone: (512) 424-2365

    b. Access and Dissemination Bureau will provide via email:
        i. the website address where you go to sign up for access to the DPS Secure Website for criminal history (FACT is a component of that site);
            1. Follow the on-site instructions
            2. Sign the Secure Site Entity Agreement and return it to DPS. You may fax the signed copies to the Access and

Dissemination Bureau and send the originals in the mail. Originals must be received within 14 days.

ii. a User Acknowledgement Agreement
    1. Sign the User Acknowledgement Agreement and return it to DPS. You may fax the signed copies to the Access and Dissemination Bureau and send the originals in the mail. Originals must be received within 14 days.

iii. The Security Policy for Non-Criminal Justice Agency Access, Use, and Dissemination of Criminal History Record Information.
    1. When you sign the User Agreement you are agreeing to abide by the Security Policy requirements.

iv. a request for the front page and signature page of your contract with a school district, open-enrollment charter school, or shared services arrangement.
    1. Please fax those documents to the Access and Dissemination Bureau and mail the originals to be mailed with the other submissions.

c. After the Agreements are received, DPS will notify you of your approval and provide you with a form (called a "Fast Fingerprint Pass") with your company's User Number for use on FACT. The form will be sent to your Message Center on the Secure Website. That form must be given to each employee who will work at a school, as described by Senate Bill 9.

2. **Perform criminal history background searches on employees who will work at a school, under the conditions described in Senate Bill 9 (listed above in *Legislative Requirement*).**

a. Direct those employees set an appointment for fingerprinting through the DPS Fingerprint Applicant Services of Texas (FAST) contractor at the phone and email listed on the *Fast Fingerprint Pass*. The person must take the *Fast Fingerprint Pass* with them to the appointment. The person will pay the fees (See Section 6, below) either at the time of scheduling or at the time of fingerprinting.

b. After the person is fingerprinted, FAST will send the fingerprints to DPS electronically. DPS will search the fingerprints through the DPS Automated Fingerprint Identification system (AFIS) which contains the fingerprints of persons reported to DPS as having been arrested in Texas. DPS will then send the fingerprints to the FBI for searching through the FBI AFIS, which contains the fingerprints of persons reported to the FBI as having been arrested in other states.

c. DPS will consolidate the results from the DPS and FBI and place them in the FACT Clearinghouse. At that time, FACT will send you an email notice that the results are available for you to review. You will sign on the FACT website to review the results and make a determination regarding the suitability of that person to work in the schools.

d. At the time that you are notified of the results, you are also automatically "subscribed" to that person's record in FACT. That means that if the person is arrested in Texas in the future, you will receive an email from FACT telling you that the person's record has been updated. (See #3 and #4, below.)

e. Senate Bill 9 requires that you "certify" to any school district at which you work that this process has been followed. The school district may ask for a person's name, driver license number, and other information to inquire into the FACT Clearinghouse and verify the results, as well.

3. **Unsubscribe to records of employees who leave your employment.**
   a. You are only authorized to see a person's criminal history as long as they are in your employ, as described in Senate Bill 9. If a person leaves your employment, you must "unsubscribe" to that record. See #4 below.
   b. The FACT website gives you an unsubscribe feature that you must use whenever a person leaves your employment. That person will remain on your FACT list of employees, but will be "inactive". If the person returns to your employment, you can simply "re-activate" the record. This is intended to assist with managing the background check requirements of seasonal employees.

4. **Respond to subscription notices of updates to the criminal history record information.**

   a. When a person to whom you are "subscribed" is reported to DPS has having been arrested in Texas, you will receive an email notification of an update to the criminal history record. You must sign into the FACT website and review the notice.

   b. Prior to viewing the updated criminal history record information, you must verify from your own records that the person is still an employee and that you are still authorized to receive the record. If the person is no longer employed by your company, you are no longer authorized to receive the updated criminal history record information.

   c. The website gives you the opportunity to review the record, or to "unsubscribe" from the record. If you are still authorized to view the record, click the appropriate button to view the record. If you are no longer authorized to view the record, click the "unsubscribe" button.

5. **Maintain Security and Confidentiality of criminal history record information obtained from FACT.**

   a. You are authorized to use the criminal history background check process only for purposes identified in Senate Bill 9. Unauthorized access to criminal history record information is a crime under Section 411.083, Texas Government Code.

   b. The FACT User Entity Agreement has a Security Policy attached. You must read and follow those guidelines.

   c. DPS will audit use of the criminal history file and of FACT. Audits will include a comparison of criminal history background check submissions from contractors against their employment records to verify that the information is only being requested and used for authorized purposes. Violations of DPS or FBI policies or state or federal law may result in termination of services and/or criminal penalties.

   d. The information in the FACT Clearinghouse is confidential, and access must be restricted to the least number of persons needed to review the records.

   e. Access to FACT must be from a computer within your company offices and cannot be from a public internet computer that is or could be shared by other users who are not authorized users within your company (for example computers in a public library).

   f. Any questions regarding the access, use, dissemination of criminal history record information must be referred to:

      Access and Dissemination Bureau
      Texas Department of Public Safety
      Crime Records Service
      P. O. Box 149322
      Austin, Texas 78714-9322

      Email: FACT@txdps.state.tx.us
      Phone: (512) 424-2365

6. Fees

1. The charge for the applicant to be fingerprinted at the FAST location is $9.95.

2. The charge for the search of the DPS criminal history file is $15.00.

3. The charge for the search of the FBI criminal history file is $19.25.

4. The total fee of $44.20 is payable in one of two methods:

    a. On-line at the time of scheduling the fingerprinting appointment. Methods of on-line payment are credit card or debit card. On-line payment requires a small (less than $2.00) convenience fee paid to the state electronic payment service. That fee is not included in the $44.20 identified above. Or:
    b. At the time of fingerprinting by personal check, cashiers check, or money order.

TEXAS DEPARTMENT OF PUBLIC SAFETY
SECURITY POLICY FOR NON-CRIMINAL JUSTICE AGENCY ACCESS, USE, AND DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

I. ACCESS BY NON-CRIMINAL JUSTICE ENTITIES

A. Legislative Authority for Non-criminal Justice Entity Access

Policy: A non-criminal justice entity legislatively authorized by Chapter 411, Subchapter F of the Texas Government Code or other Texas law to receive criminal history record information (CHRI) from the Department of Public Safety (Department or DPS) may access the DPS databases. All non-criminal justice entities granted access to the DPS CHRI will be subject to all applicable state and federal laws, rules, regulations and policies that relate to the obtaining, use and dissemination of CHRI.

The Federal Bureau of Investigation (FBI) may authorize certain Texas non-criminal justice entities access to FBI criminal history record information based upon approved Texas statutes or federal law.

Commentary: All DPS databases are maintained by the Department and may be accessed pursuant to Chapter 411, Subchapter F of the Texas Government Code or other Texas law. A non-criminal justice entity granted access to the DPS databases may submit criminal history inquiries through the DPS Access and Dissemination Bureau, Criminal History Inquiry Unit; through the DPS Secure Website for Criminal History Information; or through fingerprint submission. Results will be provided online through the DPS Secure Website, through the Fingerprint-based Applicant Clearinghouse of Texas (FACT), via the mail, or through other means, as agreed upon by DPS and the requestor. The DPS databases will provide a non-criminal justice entity only with CHRI originating in Texas. FBI requires submission of the applicants fingerprints for access to the federal records. In those instances where fingerprints are submitted under a statute approved for access to the FBI records, DPS will forward the fingerprints to the FBI and FBI will provide the record respond through the DPS.

B. Non-criminal Justice Entity User Agreements

Policy: A non-criminal justice entity requesting access to the DPS databases must provide the Department with a signed written user agreement in which the entity agrees to comply with Department policies regarding the use of the DPS databases or information. The user agreement will include standards and sanctions governing the non-criminal justice entity's utilization of the DPS databases or information and will incorporate the policies set forth in this document. These

policies also apply to access to, use, and dissemination of FBI criminal history record information, when appropriate.

Commentary: None

II. PERSONNEL SECURITY

A. Authorized Users

Policy: A non-criminal justice entity must provide the Department with the name, sex, race, date of birth, and title of each official/employee of the non-criminal justice entity who will utilize information received from the DPS databases. The Department will perform a name-based background check on each name submitted, and reserves the right to require a fingerprint-based background check, prior to approving access for the official/employee. Only those persons approved by the Department, hereinafter referred to as authorized employees, will be allowed access to the DPS databases or information on behalf of the non-criminal justice entity. An official/employee who is not approved to utilize the DPS databases or information may dispute the information forming the basis of the Department's decision through the submission of fingerprints. The Department may limit the number of authorized employees within a non-criminal justice entity. These same personnel screening criteria apply to access to the FBI criminal history record information received from the FBI through the DPS.

Commentary: Only authorized users may access the information received from the DPS and FBI databases. The number of authorized users shall be limited to the number reasonably necessary to perform criminal history checks for the purposes permitted by law.

B. User Identifier

Policy: A Department-issued user entity identifier shall be used in each transaction in the DPS databases for retrieval of CHRI.

Commentary: The Department will assign a user identifier to each non-criminal justice entity authorized by the Department to access the DPS databases for CHRI. This user identifier serves to identify the non-criminal justice entity accessing the DPS and FBI databases and ensures the proper level of access for the non-criminal justice entity.

III. FACILITY AND INFORMATION SECURITY

A. Facility Security Standards

Policy: The location of all CHRI received from the DPS or FBI databases must have adequate physical security to protect against any unauthorized viewing or access to displayed/stored/printed criminal history record information at all times.

Commentary: File cabinets or file systems used to maintain CHRI must be protected from unauthorized viewing of or access to CHRI. For example, either locking of the file cabinet or locking the access to the room the files are housed is one component of complying with this policy.

B. Information Security Standards

Policy: Criminal history record information obtained from the DPS or FBI databases is sensitive information and must be maintained in a secure records environment to prevent the unauthorized viewing or use of the criminal history record information.

Commentary: None

Policy: When retention of criminal history record information is no longer necessary or is not permitted by law, the criminal history record information shall be properly disposed. A secure manner of disposal must be utilized to destroy thoroughly all elements of the records and preclude unauthorized viewing, access or use.

Commentary: Disposal procedures should include a method sufficient to preclude recognition or reconstruction of information (i.e., shredding). The method should also provide verification that the disposal procedures were successfully completed.

IV. CRIMINAL HISTORY RECORD INFORMATION

A. Obtaining, Use and Dissemination of Criminal History Record Information

Policy:
A non-criminal justice entity may retrieve criminal history record information through the DPS or FBI databases only for legislatively authorized purposes. Criminal history record information received from the DPS or FBI databases shall be used only for legislatively authorized purposes and may not be disseminated to a person not authorized to receive the information. Upon request by the Department, all users must provide an authorized purpose for all criminal history record information inquiries. The ability to retrieve criminal history record information is subject to cancellation if the information is obtained or used in an unauthorized manner or disseminated to a person not authorized to receive the criminal history record information. Criminal sanctions are also in place for the improper obtaining, use and dissemination of criminal history record information.

Commentary: Generally, criminal history record information held by the DPS and the FBI is confidential and may be disseminated only as authorized by state or federal statute. Specific non-criminal justice entities are legislatively authorized to receive criminal history record information for limited, specified purposes. The

non-criminal justice entity is responsible for complying with all laws governing the non-criminal justice entity's access to, use, and dissemination of criminal history record information. State law makes it unlawful for a person to obtain confidential criminal history record information in an unauthorized manner, use the information for an unauthorized purpose, or disclose the information to a person not entitled to the information. State law also makes it unlawful for a non-criminal justice entity to provide a person with a copy of the person's criminal history record information obtained from the Department unless authorized to do so by a specific state statute.

B. **Commercial Dissemination**

Policy: The commercial dissemination of criminal history record information obtained from the DPS or FBI databases is prohibited.

Commentary: The marketing of data for profit is not permitted. State law makes it a felony offense to obtain, use, or disclose, or employ another to obtain, use or disclose, criminal history record information for remuneration or for the promise of remuneration.

V. AUDITS

A. **Security Audits**

Policy: A security audit may be performed on a periodic basis by the Department or FBI for the purpose of measuring the non-criminal justice entity's compliance with the laws, rules, regulations and policies relating to the DPS databases and the criminal history record information obtained there-from.

TEXAS DEPARTMENT OF PUBLIC SAFETY
CRIME RECORDS SERVICE

SIGNATURE REQUIRED

Please print, sign and mail the signed user agreement and primary user acknowledgement to DPS (Address at bottom)

All signatures must be signed in blue ink

"Access" is defined as physical access: The ability to receive, view, or discuss the Criminal History Record Information (CHRI) regardless of retrieval method from Texas Department of Public Safety.	**Date:** **Application ID:**

DPS Criminal History and Fingerprint-based Applicant Clearinghouse of Texas User Entity Agreement

1. This document constitutes an agreement between the Texas Department of Public Safety (DPS), Administrator of the Texas Secure Website for Criminal Record History Information, the Fingerprint-based Applicant Clearinghouse of Texas (FACT) and the state criminal history record information repository, and

Entity Name _____

User Contact Name _____

User Contact Address _____

User Contact Email _____

Phone _____

an authorized agency or qualified entity legislatively authorized to retrieve state and federal criminal history record information (CHRI), hereinafter referred to as the User Entity.

2. This Agreement sets forth the duties and responsibilities of the Department of Public Safety and the User Entity.

3. Under this agreement, the Department of Public Safety agrees to provide and manage access to DPS and Federal Bureau of Investigation criminal history record information via the Secure Website for Criminal History Record Information, the Fingerprint-based Applicant Clearinghouse of Texas and any other method of access to CHRI. The User Entity shall not permit any person or entity, other than the User Entity's authorized employees, to retrieve CHRI under this agreement. The Department of Public Safety will perform a name-based criminal history check, and reserves the right to require a fingerprint-based criminal history check, on authorized employees of the User Entity prior to allowing them to retrieve information.

4. The Department of Public Safety will provide an electronic subscription service to User Entities with access to the FACT to provide notice of updates to CHRI contained within the FACT. The Department of Public Safety will only provide notice of updates if the User Entity is a subscriber to the record. DPS will provide the User Entity with the option to view the updated record, or to unsubscribe if the User Entity is no longer authorized to access CHRI relating to the subject.

5. The User Entity may retrieve CHRI under this agreement only for those purposes permitted by state and federal law. Any use of CHRI retrieved under this agreement shall be limited to those uses permitted by state and federal law.

6. No financial liability will be incurred by the Department of Public Safety by virtue of this agreement beyond monies available to it for the purpose of fulfilling this agreement.

7. The User Entity and its employees shall abide by all present and hereafter enacted state and federal laws, rules and regulations concerning the collection, storage, retrieval, use, destruction, disclosure and dissemination of CHRI. The User Entity shall provide the subject of the CHRI the opportunity to complete, or challenge the accuracy of, the information contained in the state and federal CHRI. The procedures for obtaining a change, correction, or updating of FBI records are set forth in 28 CFR 16.34. The Error Resolution Unit of the Texas Department of Public Safety, Crime Records Service, processes challenges to the completeness or accuracy of DPS records as provided by 37 Texas Administrative Code Section 27.1(d).

8. The User Entity shall be responsible for ensuring that the User Entity and its employees accessing criminal history record information under this agreement are informed of all applicable state and federal laws, rules and regulations concerning the collection, storage, retrieval, use, destruction, disclosure and dissemination of CHRI. The User Entity shall promptly notify the Department of Public Safety of a violation by the User Entity, or by an employee of the User Entity, of any applicable state or federal law, rule or regulation relating to the collection, storage, retrieval, use, destruction, disclosure or dissemination of criminal history record information retrieved under this agreement.

9. The Department of Public Safety reserves the right to immediately suspend service to the User Entity when the Department determines that this agreement or any applicable state or federal law, rule or regulation has been violated by the User Entity or an employee of the User Entity. The Department of Public Safety may reinstate service following such instances upon receipt of satisfactory assurances that such violations have been corrected and measures have been taken to prevent future violations. The Department of Public Safety shall have the authority to inspect and audit the equipment, records and operations of the User Entity to determine compliance with this agreement and all applicable state and federal laws.

10. Either the Department of Public Safety or the User Entity may, upon 30 days written notice, discontinue service. The Department of Public Safety shall not be required to give notice prior to suspending service as stated above in paragraph 9.

11. The User Entity agrees to hold harmless the Texas Department of Public Safety, its Director and employees from and against any and all claims, demands, actions and suits, including but not limited to, any liability for damages by reason of or arising out of any negligence on the part of the User Entity or its employees with regard to the collection, storage, retrieval, use, destruction, disclosure or dissemination of CHRI retrieved under this agreement.

12. Any employee, applicant, volunteer, or volunteer applicant who will be accessing the DPS Criminal History databases or information shall be subject to a criminal history background check. If a felony conviction of any kind exists, access to the system shall be denied. A review of the denial may be requested in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance. If a record of any other kind exists, systems access shall not be granted until further review of the matter is determined to verify if systems access is appropriate. If the person

appears to be a fugitive or appears to have an arrest history without conviction for a felony or serious misdemeanor, the person shall be under review to determine if systems access is appropriate. If, after review, a determination is made that systems access by the person would not be in the public interest, access shall be denied and the User Entity shall be notified in writing of the denial.

13. Any support personnel, contractors, and custodial workers who access CHRI areas shall be subject to a criminal history background check, as described in paragraph #12, unless these individuals are escorted by authorized personnel at all times. Authorized personnel are those persons who have passed a name-based record check or a fingerprint-based check and have been granted access.

14. The criminal history record information accessed under this agreement is sensitive and security measures must be taken to prevent any unauthorized access, use, or dissemination of the information. Any improper access, use, or dissemination of CHRI may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

15. The User Entity and its employees accessing criminal history record information under this agreement have read and agree to abide by the Texas Department of Public Safety *Security Policy for Non-criminal Justice Agency Access, Use, and Dissemination of Criminal History Record Information* attached to this agreement and incorporated herein by reference.

In WITNESS WHEREOF, the parties hereto caused this agreement to be executed by the proper officers and officials.

USER ENTITY

Signature: _____

Printed Name: _____

Title: _____

Date: _____

PLEASE MAIL TO:

DEPARTMENT OF PUBLIC SAFETY
CRIME RECORDS SERVICE
PO BOX 149322
AUSTIN TX 78714-9322

OFFICIAL USE ONLY. PLEASE DO NOT WRITE IN THE BOX BELOW.

TEXAS DEPARTMENT OF PUBLIC SAFETY

By: _____

Title: _____

Date: _____

TEXAS DEPARTMENT OF PUBLIC SAFETY
CRIME RECORDS SERVICE

Please sign in blue ink and mail to DPS

(Address at end of this document)

Authorized User Acknowledgement

• Authorized users approved by the Department to use the criminal history record information (CHRI) have regular access to confidential criminal history information as a part of their job duties.

• All authorized users must clearly understand that any unauthorized retrieval, use or dissemination of this confidential information is a violation of state law and can lead to the filing of criminal charges against the authorized user, in addition to cancellation of access to the Department of Public Safety (DPS) databases. Following is a copy of Texas Government Code Section 411.085, which describes the criminal penalties related to unauthorized retrieval, use, or dissemination of criminal history record information:

§ 411.085. Unauthorized Obtaining, Use, or Disclosure of Criminal History Record Information; Penalty

a. A person commits an offense if the person knowingly or intentionally:
    1. obtains criminal history record information in an unauthorized manner, uses the information for an unauthorized purpose, or discloses the information to a person who is not entitled to the information;
    2. provides a person with a copy of the person's criminal history record information obtained from the department; or
    3. violates a rule of the department adopted under this subchapter.
b. An offense under Subsection (a) is a Class B misdemeanor, except as provided by Subsection (c).
c. An offense under Subsection (a) is a felony of the second degree if the person:
    1. obtains, uses, or discloses criminal history record information for remuneration or for the promise of remuneration; or
    2. employs another person to obtain, use, or disclose criminal history record information for remuneration or for the promise of remuneration.