

Persons Ineligible for Hire

The District is prohibited by law from hiring an applicant for employment who is listed on the Texas Education Agency's registry of persons not eligible for employment by a school district.

Criminal History Review

The District will conduct a criminal history record review for a final candidate for employment and will determine through the individualized assessment procedures described below whether the individual should be excluded from employment. [See DBAA(LOCAL)]

Only District employee(s) authorized to view criminal history records will be involved in conducting an individualized criminal history record review.

Notice to Candidate for Employment

Claim of Error in Records

A candidate for employment who has a criminal history record will be notified in writing that he or she may be excluded from employment due to criminal history. The candidate will be given an opportunity to provide additional information concerning his or her criminal history record to be considered as part of the individualized assessment process.

Additional information may include:

- Documentation showing inaccuracies in the criminal record;
- Any evidence related to the factors for individualized assessment listed at DBAA(LOCAL);
- Evidence that he or she has performed the same type of work since the incident(s) noted on the criminal history record, with no known incidents of criminal conduct;
- Rehabilitation efforts, including education and training;
- Employment or character references; and
- Whether or not he or she is bonded (if a bond is required for the job position with the District).

If the individual does not provide additional information in a timely manner, the District will proceed with an individualized determination with the information available to the District.

A candidate for employment who claims that the reported criminal history record is erroneous may be provided a copy of the record so that he or she can undertake efforts to correct the record.

Individualized Assessment

In conducting the individualized assessment, the District will consider both the factors described in DBAA(LOCAL) and any additional information provided by the individual. The District may obtain court records, if needed, to validate the information provided.

Using the available information, the District will determine whether or not exclusion from employment is consistent with business necessity.

Offenses for Which Exclusion Is Likely

A record of certain offenses carries a high likelihood that the District will exclude the individual from employment. Subject to an individualized assessment, the following classes of offense will likely preclude employment with the District:

- Any offense requiring exclusion pursuant to Education Code 22.085.
- Any offense for which employment of the individual places the safety of both students and other employees at risk regardless of the date of the offense, its relation to the employee's job, or the age of the victim. Such offenses include homicide, murder, capital murder, unlawful transport, false imprisonment, trafficking of persons, improper relationship between educator and student, sexual assault, aggravated sexual assault, rape, child abuse, sale or purchase of a child, arson, robbery, aggravated robbery, prostitution or solicitation of prostitution, child pornography, and sexual solicitation of a child.
- Any offense that, because of the relationship between the offense and the duties and responsibilities of the position in question, creates a risk to the best interests of the District. For example, a person who has committed a property offense will not normally be eligible for a position with financial duties or responsibilities.
- Any felony conviction that occurred within the ten years prior to application for employment with the District.
- Any Class C misdemeanor conviction involving moral turpitude within the ten years prior to application for employment with the District. [For the purposes of this regulation and related procedures, the definition of moral turpitude is found at DH(LOCAL).]

Adjudication of Offenses

In considering the adjudication of the offense, the following standards apply.

Conviction

The District will ordinarily treat a conviction as proof of guilt. A conviction record constitutes reliable evidence that a person engaged in the criminal conduct "beyond a reasonable doubt."

Arrest

An arrest record alone does not establish criminal conduct. Before the District makes an employment decision based on an arrest, the District will examine the circumstances surrounding the arrest and

will make any necessary inquiries. The District is not required to conduct an extensive investigation to determine the individual's guilt or innocence but need only make inquiries that could shed light on the likelihood of the individual's guilt in committing the underlying offense.

An arrest will be treated as a conviction when inquiries suggest a high likelihood that the individual committed the underlying offense. Where such a determination is not found, the arrest will not be used to take an adverse employment action against the individual.

*Deferred
Adjudication*

A grant of deferred adjudication resulting from a no contest or guilty plea will ordinarily be treated as an admission of guilt. However, the District will make inquiries similar to the inquiries made when an arrest is reported.

When such inquiries suggest a high likelihood that the individual committed the underlying offense, deferred adjudication will be treated as a conviction. Where such a determination is not found, deferred adjudication will not be used to take an adverse employment action against the individual.

*Not Guilty,
Withdrawn, or
Dismissed
Charges*

For a not guilty, withdrawn, or dismissed adjudication, the individual will be asked to explain, in writing, the circumstances and must provide a certified copy of the court paperwork showing the final disposition of every charge. The District may make additional inquiries into the surrounding circumstances.

The charges will be treated as a conviction when such inquiries suggest a high likelihood that the individual committed the underlying offense. Where such a determination is not found, the criminal history in question will not be used to take an adverse employment action against the individual.

Types of
Convictions

If the criminal history record shows a conviction, or if inquiries made during the record review indicate a high likelihood of guilt and/or recurrence, then the following employment restrictions will apply.

Felony

For a felony offense committed within the ten years before application for employment, see Offenses for Which Exclusion Is Likely, above.

If the individual committed a felony offense more than ten years before application for employment, the District will determine whether the conviction was for an offense that generally requires exclusion by law or by policy or, if not, whether the underlying offense relates to the duties and responsibilities of the desired position.

The following guidelines will apply:

- If the offense does not relate to the duties and responsibilities of the position and was not for an offense that would otherwise preclude employment, the individual may be considered for employment or continued employment.
- If the offense does relate to the duties and responsibilities of the position, the District will consider the likelihood of recurrence of the criminal behavior. A determination that the behavior is unlikely to recur will result in the individual being eligible for employment; a finding to the contrary will result in the individual being ineligible for employment.

*Class A and B
Misdemeanors*

An individual may be eligible for employment if the conviction for a Class A or Class B misdemeanor is not related to the duties and responsibilities of the position and/or has occurred more than five years prior.

If the conviction occurred in the past five years and does relate to the duties and responsibilities of the position, and if it is determined there is a high degree of likelihood for the recurrence of the behavior, the employee is ineligible for employment in the District.

*Class C
Misdemeanors*

For a Class C misdemeanor offense involving moral turpitude committed within the ten years before application for employment, as applicable, see Offenses for Which Exclusion is Likely, above.

If convicted of a Class C misdemeanor that does not involve moral turpitude or that occurred more than ten years before application of employment, the District will determine whether the underlying offense relates to the duties and responsibilities of the desired position.

The following guidelines will apply:

- If the offense does not relate to the duties and responsibilities of the position and was not for an offense that would otherwise preclude employment, the individual may be considered for employment.
- If the offense does relate to the duties and responsibilities of the position, the District will consider the likelihood of recurrence of the criminal behavior. A determination that the behavior is unlikely to recur will result in the individual being eligible for employment; a finding to the contrary will result in the individual being ineligible for employment.

Multiple Offenses

An individual with multiple offenses that individually do not make him or her ineligible for employment may be deemed ineligible for

continued employment when repetitious criminal behavior indicates a high degree of likelihood for recurrence of the behavior.

Unlisted Criminal History

If a criminal history record does not list an event reported by the candidate for employment, he or she will be asked to explain, in writing, the circumstances for each reported incident. A certified copy of pertinent court paperwork showing final disposition of the charge must be included. The District may make additional inquiries.

Note: In addition to a signed user agreement with the Department of Public Safety (DPS), a criminal or non-criminal justice agency, such as the school district, that receives criminal history record information (CHRI) from DPS under Government Code Chapter 411, Subchapter F, or other state or federal law, must develop written procedures concerning access to and use of CHRI. The sample procedures below contain requirements outlined in the [DPS security policy](#)¹ and may be amended to reflect additional District procedures.

The Texas Dept of Public Safety's Documents website has further information regarding the handling of criminal history record information in accordance with federal standards, including the [Criminal Justice Information Services \(CJIS\) Security Policy, companion documents, and sample forms](#).² For more information on the federal regulation concerning criminal history information, see [28 C.F.R. Part 20](#).³

Additional resources, including a training module overview and a sample training email to personnel, are available at [CJIS Security Awareness Training](#)⁴ on the Texas Department of Public Safety's website.

Criminal History Record Information

Scope

The following provisions apply to any electronic or physical media containing Federal Bureau of Investigation criminal justice information (CJI) and its subset, criminal history record information (CHRI), as defined at DBAA(LEGAL). CJI and CHRI have the same meaning for the purpose of this regulation and will be interpreted to include any information that could potentially be considered CJI or CHRI.

CJI includes biometric, identity history, biographic, property, and case/incident history data and information obtained from the Interstate Identification Index.

These provisions also apply to any authorized person who accesses, stores, and/or transports electronic or physical media.

Point of Contact The District designates the _____ (*position title, e.g., human resources director, information officer, or police chief*) as the point of contact (POC) who will oversee compliance with the user agreement and all aspects of CHRI security.

Proper Access, Use, and Dissemination of CHRI Only authorized District personnel will access CHRI, and only for authorized purposes. Authorization may only be granted in compliance with Texas Department of Public Safety (DPS) policies or other conditions of access set by information-granting agencies.

Authorized Personnel The District will conduct a national fingerprint-based record check for all personnel, within 30 days of employment or assignment if practicable, who have been granted direct access to CHRI, those who have direct responsibility for configuring and maintaining computer systems and networks with direct access to CHRI, and any persons with access to physically secure locations or controlled areas containing CHRI.

Note: Districts that contract with information technology or human resources service providers to manage activities such as hiring, records retention, media destruction, or document destruction should review [crime records](#)⁵ on the DPS website. to review the Outsourcing Standards and develop regulations regarding these contractors' handling of CHRI.

Security Awareness Training The District will require basic security awareness training within six months of initial hire or assignment for all personnel who have access to CHRI. Thereafter, the District will require basic security awareness training every two years. The District will document and retain records of all training.

Physical Security CHRI will be kept in a location with physical and personnel security controls sufficient to protect the CHRI and associated information systems from unauthorized viewing or access. The perimeter of the physically secure location will be prominently posted and separated from nonsecure locations by physical controls.

Only authorized personnel will have access to the physically secure locations. The District will maintain and keep current a list of authorized personnel. The District will implement access controls and monitor physically secure areas to protect all transmission and display media of CHRI. Authorized personnel will take necessary steps to prevent physical, logistical, and electronic breaches.

<i>Media Protection</i>	<p>The District will put controls in place to protect electronic and physical media containing CHRI while at rest, in storage, in transit, or in use. Electronic media include memory devices in laptops and computers, such as hard drives, and any removable, transportable digital memory medium, such as a magnetic tape or disk, backup medium, optical disk, flash drive, external hard drive, or digital memory card. Physical media include printed documents and imagery that contain CHRI.</p> <p>The District will securely store electronic and physical media within physically secure locations or controlled areas. The District will restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible, then the data will be encrypted as described in the CJIS Security Policy.</p>
<i>Media Transport</i>	<p>The District will put controls in place to protect electronic and physical media containing CHRI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. The District will protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.</p>
Sanitation and Disposal of CHRI	<p>In accordance with the District's records control schedules and any other procedures established by the District, the District will properly dispose of hard drives, diskettes, tape cartridges, CDs, printer ribbons, hard copies, printouts, and other similar items used to process, store, and/or transmit CHRI.</p>
<i>Physical Media</i>	<p>Physical media such as printouts will be disposed of by one of the following methods:</p> <ul style="list-style-type: none">• Shredding using District shredders;• Placement in locked shredding bins for an authorized shredding contractor to come to District premises and shred, witnessed by District personnel throughout the entire process; or• Incineration using District incinerators or by an authorized incineration contractor, witnessed by District personnel either at a District or contractor incineration site.
<i>Electronic Media</i>	<p>The District will dispose of electronic media, such as hard drives, tape cartridges, CDs, printer ribbons, or printer and copier hard drives, using one of the following methods:</p> <ul style="list-style-type: none">• Overwriting at least three times. Overwriting uses a program to write binary code onto the location of the file needing sanitization.

- Degaussing. Degaussing magnetically erases data from magnetic media, using strong magnets or electric degaussers.
- Destruction. Destruction involves physically dismantling electronic media by methods such as crushing or disassembling, ensuring that the platters have been physically destroyed so that no data can be retrieved.

Information technology systems that have been used to process, store, or transmit CHRI will not be released from the District's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account
Management

The District will manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The District will validate information system accounts at least annually and will document the validation process.

All accounts will be reviewed at least annually by the POC or designee to ensure that access to and account privileges on systems that contain CHRI are commensurate with job functions, need-to-know, and employment status. The POC may also conduct periodic reviews.

Remote Access

The District will authorize, monitor, and control all methods of remote access by eligible employees to the information systems that can access, process, transmit, and/or store CHRI. Remote access is any temporary access to the District's information system by a user (or an information system) communicating temporarily through an external, non-District-controlled network (e.g., the internet).

The District will employ automated mechanisms to facilitate the monitoring and control of remote access methods. The District will control all remote accesses through managed access control points. The District may permit remote access for privileged functions only for compelling operational needs but will document the rationale for such access in the security plan for the information system.

Publicly Accessible
Computers

Utilizing publicly accessible computers to access, process, store, or transmit CHRI is prohibited. Publicly accessible computers include hotel business center computers, convention center computers, public library computers, and public kiosk computers.

Personally Owned
Information
Systems

A personally owned information system will not be authorized to access, process, store or transmit CHRI unless the District has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes any portable technology, such as a camera, USB flash

	<p>drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops, or any personal desktop computer. If bring-your-own-devices (BYOD) are authorized, they will be controlled using the requirements described in the most recent CJIS Security Policy.</p>
Reporting Information Security Events	<p>The District will promptly report incident information to appropriate authorities, including the DPS. Information security events and weaknesses associated with information systems will be communicated in a manner allowing timely corrective action to be taken and notifications be issued in accordance with law and Board policy.</p> <p>Formal event reporting and escalation procedures will include:</p> <p><i>[Describe your formal process for event reporting and escalation procedures. Include all appropriate information about the level of reporting and any time frames for reporting an event.]</i></p> <p>Wherever feasible, the District will employ automated mechanisms to assist in the reporting of security incidents.</p> <p>The District will make all employees, contractors, and third-party users aware of the procedures for reporting different types of events and weaknesses that might have an impact on the security of District assets and are required to report to the designated POC any information security events and weaknesses.</p> <p>If the incident involves unauthorized use of or access to the District's cyberinfrastructure or to sensitive personal information or student information constituting a breach of system security as defined by law, the incident must be reported in accordance with the District's cybersecurity plan. [See CQB]</p>
Violations or Misuse	<p>Violation by an employee of any requirements of DBAA(LEGAL), DBAA(LOCAL), DBAA(REGULATION), or the most recent CJIS Security Policy may result in suitable disciplinary action, up to and including loss of access privileges, termination, and/or civil or criminal prosecution.</p> <p>Violation by a visitor of any requirements of DBAA(LEGAL), DBAA(LOCAL), DBAA(REGULATION), or the most recent CJIS Security Policy may result in suitable disciplinary action against the sponsoring employee, up to and including loss of access privileges, termination, and/or civil or criminal prosecution.</p>

¹ DPS: Security Policy: <https://secure.txdps.state.tx.us/dpswebsite/criminalhistory/SecurityPolicy.aspx>

² DPS: Documents: <https://www.dps.texas.gov/SecurityReview/documents.htm>

³ 28 C.F.R. Part 20 : <https://www.govinfo.gov/content/pkg/CFR-2010-title28-vol1/pdf/CFR-2010-title28-vol1-part20.pdf>

⁴ DPS: CJIS Security Awareness Training: <https://www.dps.texas.gov/SecurityReview/secAwareness.htm>

⁵ DPS: Crime Records: https://www.dps.texas.gov/administration/crime_records/pages/index.htm