Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

(Proper Access, Use and Dissemination Procedures)

Purpose

The Board of Education's (Board) intent of this policy is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until the information is purged or destroyed in accordance with applicable record retention rules.

This policy is based upon the FBI's Criminal Justice Information Services (CJIS) Security Policy. The Board considers the FBI CJIS Security Policy as the minimum standard. This Board policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope

This policy applies to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location within the District. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)

CJI refers to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

CHRI is a subset of CJI and for the purposes of this policy is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

Proper Access, Use, and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Proper Access, Use, and Dissemination of CHRI (continued)

Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

Personnel Security Screening

Access to CJI and/or CHRI is restricted to authorized personnel. Authorized personnel is defined as an individual or group of individuals, appropriately vetted through a national fingerprint-based record check and granted access to CJI data. Agencies, including school districts, located within states with legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to CHRI for the purposes of licensing or employment shall submit a fingerprint-based record check within 30 days of employment or assignment on all personnel with those who have direct access to CJI, those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI, and any persons with access to physically secure locations or controlled areas containing CJI.

Security Awareness Training

Basic security awareness training is required, within six months of initial assignment, and biennially thereafter, for all personnel with access to CJI.

Physical Security

A “physically secure location” is a facility or an area, room, or group of rooms within a facility with sufficient physical and personnel security controls to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

Only authorized personnel shall access physically secure non-public locations. The District will maintain a current list of authorized personnel. All physical access points into the District’s secure areas will be authorized before granting access. The District will implement access controls and monitor physically secure areas to protect all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the District from physical, logical and electronic breaches.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI) (continued)

Media Protection

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

The District shall securely store electronic and physical media within physically secure locations or controlled areas. The District restricts access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

Media Transport

Controls shall protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. The District shall 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.

Media Sanitization and Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI shall be properly disposed of in accordance with measures established by the District.

One of the following methods shall dispose of physical media (printouts and other physical media):

1. Shredding using District issued shredders;
2. Placed in locked shredding bins for private contractor to come on-site and shred, witnessed by District personnel throughout the entire process;
3. Incineration using District incinerators or witnessed by District personnel onsite at District or at contractor incineration site, if conducted by non-authorized personnel.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Media Sanitization and Disposal (continued)

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the following District methods:

1. *Overwriting* (at least 3 times) – an effective method of clearing data from magnetic media. Overwriting uses a program to write (1's, 0's, or a combination of both) onto the location of the media where the file to be sanitized is located.
2. *Degaussing* – a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Common magnets are weak and shall not be used to degauss magnetic media.
3. *Destruction* – a method of destroying magnetic media. Destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall 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 shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The District shall validate information system accounts at least annually and shall document the validation process.

All accounts shall be reviewed at least annually by the designated CJIS point of contact (POC) or his/her designee to ensure that access and account privileges are commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The POC may also conduct periodic reviews.

Remote Access

The District shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. 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).

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Remote Access (continued)

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

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Personally Owned Information Systems

A personally owned information system is not authorized to access, process, store or transmit CJI 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 like camera, USB flash 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.

Reporting Information Security Events

The District shall promptly report incident information to appropriate authorities to include the state CSA or SIB's Information Security Officer (ISO). Information security events and weaknesses associated with information systems shall be communicated to allow for timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the District shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Policy Violation/Misuse Notification

Violation of any of the requirements contained in this CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Policy Violation/Misuse Notification (continued)

Likewise, violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any visitor can result in similar disciplinary action against the sponsoring employee, and can result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

(cf. 4112.5/4212.5 - Security Check/Fingerprinting)
(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181 and June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67)

29-17a Criminal history checks. Procedure. Fees.

PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

CJIS Security Policy

Title 28 C.F.R. Part 20

Policy adopted: November 7, 2017

NEWTOWN PUBLIC SCHOOLS
Newtown, Connecticut

Personnel – Certified/Non-Certified

Security Check/Fingerprinting

Each person hired by the school system shall be required to submit to state and national criminal record checks. In order to process such record checks, the following procedure will be followed:

1. No later than ten calendar days after the Superintendent or his/her designee has notified job applicant of a decision to hire the applicant, or as soon thereafter as practicable, the Superintendent or his/her designee will supply the applicant with a packet containing all documents and materials necessary for the applicant to be fingerprinted. This packet shall also contain all documents and materials necessary to submit the completed fingerprints to the State Police Bureau of Identification for the processing of state and national criminal record checks.
2. No later than ten calendar days after the Superintendent or his/her designee has provided the successful job applicant with the fingerprinting packet, the applicant must arrange to be fingerprinted. Failure of the applicant to have his/her fingerprints taken within such ten-day period, without good cause, will be grounds for the withdrawal of the offer of employment.
3. Any person for whom criminal records checks are required to be performed pursuant to this policy must pay all fees and costs associated with the fingerprinting process and/or the submission or processing of the requests for criminal record checks.
4. Upon receipt of a criminal record check indicating a previously undisclosed conviction, the Superintendent or his/her designee will notify the affected applicant/employee of the results of the record check and will provide an opportunity for the affected applicant/ employee to respond to the results of the criminal record check.
5. Decisions regarding the effect of a conviction upon an applicant/employee, whether disclosed or undisclosed by the applicant/employee, will be made on a case-by-case basis. Notwithstanding the foregoing, the falsification or omission of any information on a job application or in a job interview, including, but not limited to information concerning criminal convictions or pending criminal charges, shall be grounds for disqualification from consideration for employment or discharge from employment.
6. Each applicant for a position involving direct student contact is required to make three disclosures to the Board for a position involving direct student contact. The applicant must:
    a. Provide the District with contact information for current and former employers if they were education employers or the employment otherwise involved contact with children. The contact information must include each employer's name, address, and telephone number.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

b. Provide a written authorization that consents to and authorizes such former employers to disclose information and related records about him or her that is requested on the SDE-designed standardized form that interviewing education employers send. The authorization also must consent to and authorize SDE to disclose information and related records to requesting education employers and release such former employers and SDE from any liability that may arise from such disclosure or release.

c. Give a written statement about whether he or she:

. was the subject of an abuse or neglect or sexual misconduct investigation by any employer, state agency, or municipal police department, unless the investigation resulted in a finding that all allegations were unsubstantiated;

ii. was disciplined or asked to resign from a job or resigned from or otherwise separated from any job while an allegation of abuse or neglect was pending or under investigation by the Department of Children and Families (DCF), or an allegation of sexual misconduct was pending or under investigation or because of an allegation substantiated by DCF of abuse or neglect or sexual misconduct or a conviction for abuse or neglect or sexual misconduct; or

iii. had a professional or occupational license or certificate suspended or revoked or ever surrendered one while an allegation of abuse or neglect was pending or under investigation by DCF, or an investigation of sexual misconduct was pending or under investigation, or because of an allegation substantiated by DCF of abuse or sexual misconduct or a conviction for abuse or sexual misconduct.

7. The District is prohibited from offering employment for any position involving direct student contact until the following has occurred:

a. the applicant has complied with the above disclosure requirements;

b. the District has reviewed, either through written or telephone communication, the applicant's employment history on the standardized form filled out by current and past employers, which current or former employers must complete and return within five business days of receipt; and

c. the District has requested information from SDE about the applicant's eligibility status for a position requiring a certificate, authorization, or permit; previous disciplinary action for a substantiated finding of abuse or neglect or sexual misconduct; and notice of a criminal conviction or pending criminal charges against the applicant.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

8. A good faith effort to reach an applicant's current and previous employers shall be made. A "good faith effort" is one requiring no more than three phone calls on three separate days.

9. The District may request additional information from an applicant's current or former employers relating to any response the applicant listed on the standardized SDE form, to which the applicant must respond within five business days of receipt. Immunity is provided from criminal and civil liability to any employer who provides such information, as well as to SDE, as long as the information supplied is not knowingly false.

10. The information available to the Board from SDE about an applicant may include:

    a. any information about the applicant's eligibility for employment with such education employer in a position that requires a certificate, authorization, or permit;

    b. whether SDE knows if the applicant was disciplined for a finding of abuse or neglect or sexual misconduct, and any information related to the finding; and

    c. whether SDE has been notified that the applicant has been convicted of a crime or of pending criminal charges against the applicant and any information about such charges.

11. A substitute teacher who is hired by the district must submit to state and national criminal history record checks according to the procedures outlined above, subject to the following:

    a. If the state and national criminal history record checks for a substitute teacher have been completed within one year prior to the date the district hired the substitute teacher, and if the substitute teacher arranged for such prior criminal history record checks to be forwarded to the Superintendent, then the substitute teacher will not be required to submit to another criminal history record check at the time of such hire.

    b. If a substitute teacher submitted to state and national criminal history record checks upon being hired by the district, then the substitute teacher will not be required to submit to another criminal history record check so long as the substitute teacher is continuously employed by the district, that is, employed for at least one day of each school year, by the district, provided a substitute teacher is subjected to such checks at least once every five years.

12. Adult Education teachers, if they are continuously employed by the district, that is, employed for a least one day of each school year by the district, do not have to be fingerprinted after fulfilling the initial requirement.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

13. The District shall maintain a list of individuals suitable to work as substitute teachers. Only those on the list may be hired as substitute teachers. An individual remains on the list as long as (1) he or she is continuously employed by the District as a substitute teacher and (2) District does not have any knowledge that would cause the person to be removed from the list.

14. School nurses and nurse practitioners appointed by the Board or under contract with the Board shall also submit to a criminal history check pursuant to C.G.S. 29-17a.

15. Student teachers placed in District schools as part of completing preparation requirements for the issuance of an educator certificate shall also submit to a criminal history check. The criminal history check shall be done prior to being placed in a school for clinical experiences such as field experiences, student teaching or internship. Candidates may be fingerprinted at one of the RESCs or through local police stations or the school district. The District is required to notify the State Board of Education if notice is received that a student teacher has been convicted of a crime.

16. Each applicant for a certified position must submit to a records check of the Department of Children and Families (DCF) Child Abuse and Neglect Registry established pursuant to C.G.S. 17a-101k before the applicant may be hired. The Superintendent or his/her designee shall request the required records check of DCF in accordance with the procedures established by DCF.

17. Each applicant for a non-certified position must submit to a records check of the Department of Children and Families (DCF) Child Abuse and Neglect Registry established pursuant to C.G.S. 17a-101k before the applicant may be hired. The Superintendent or his/her designee shall request the required records check of DCF in accordance with the procedures established by DCF.

18. Contractors that apply for positions involving direct student contact are required to perform the checks on their employees who would fill such positions. These checks are similar to the ones the District must perform on applicants.

    a. A contractor's employee must fulfill the three disclosure requirements that a regular, direct applicant for such a position must fulfill.
    b. The contractor must contact any current or former employers that were education employers and request, by telephone or in writing, any information about whether there was a finding of abuse or neglect or sexual misconduct against the employee, and which the employer must report if there is one.
    c. Should the contractor receive any information indicating such a finding or otherwise has knowledge of one, he or she must immediately forward, either by telephone or in writing, the information to the District.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

d. The District must determine whether the employee may work in a position involving direct student contact at any of its schools.

e. It is not considered a breach of contract for the District to determine that the contractor's employee is forbidden to work under any such contract in such a position.

19. The District shall notify SDE when it receives information that applicants or employees have been disciplined for a finding of abuse or sexual misconduct.

20. The District is required to provide upon request, to any other education employer or to the Commissioner of Education, information it may have about a finding of abuse or sexual misconduct for someone being vetted for hire as a direct employee of the Board or a contractor's employee.

21. The Board is prohibited from entering into any collective bargaining agreement, employment contract, resignation or termination agreement, severance agreement, or any other agreement or take any action that results in any of the following outcomes:
    a. has the effect of suppressing information about an investigation of a report of suspected abuse or neglect or sexual misconduct by a current or former employee;
    b. affects the education employer's ability to report suspected abuse or neglect or sexual misconduct to appropriate authorities; or
    c. requires the district to expunge information about an allegation or finding of suspected abuse or neglect or sexual misconduct from any documents it maintains, unless after investigation the allegation is dismissed or found to be false.

22. The District may employ or contract with an applicant for up to 90 days while awaiting the complete review of their application information, as long as the following has occurred:
    a. the applicant has submitted to the District the three required disclosures,
    b. the District has no information about the applicant that would disqualify him or her from employment, and
    c. the applicant affirms that he or she is not disqualified from employment with the education employer.

23. Applicants who knowingly provide false information or knowingly fail to disclose information that is statutorily required to the District is subject to discipline by the District. Such discipline may include denial of employment or termination of a certified employee's contract.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Criminal Justice Information*

Policies #4112.5/4212.5 and #4112.51/4212.51 and applicable law require applicants for employment in the District to submit to state and national criminal record checks. All results for such background checks and accompanying information is considered "Criminal Justice Information (CJI)." Such information is to be maintained, used and disclosed in compliance with this administrative regulation. These regulations apply to all CJI that the District possesses or controls in any form or format, including CJI contained in correspondence, documentation or reports of the District.

Definitions

Criminal Justice Information (CJI) means the results of any state or federal criminal record checks of an applicant for employment in the district, volunteer, employee, or contractor and all copies thereof.

Criminal Justice Information Officer (CJI Officer) means the individual appointed by the Superintendent to be responsible for the use, disclosure, and safeguarding of CJI in the District. This individual serves as the District's primary point of contact for CJI matters and these regulations.

Permitted Individual means an individual designated by the Superintendent, or his/her designee, who may access CJI. Such individuals may include, but are not limited to, human resources personnel, and certain administrative staff.

Request and Use of Criminal Justice Information

An employee, contractor, applicant, volunteer, will be asked by the District for CJI as permitted or required by applicable policy and/or law.

The Superintendent or his/her designee shall designate those individuals who will be considered "Permitted Individuals" for purposes of these regulations. CJI may not be accessed by any other member of the District staff or be used for any reason without obtaining prior written approval from the CJI Officer. CJI used by the "Permitted Individual" is limited to that permitted or required by law or District policy.

"Permitted Individuals" must satisfy applicable legal screening requirements prior to access to CJI, including the following:

1. Permitted Individuals who are Connecticut residents shall be screened by the District through a Connecticut and national fingerprint-based record check after designations as a Permitted Individual.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

2. Permitted Individuals who are not Connecticut residents shall be subject to a District state and national fingerprint-based record check and follow FBI guidance pertaining to additional screening requirements.

The Connecticut Department of Emergency Services and Public Protection may be consulted by the CJI Officer pertaining to the execution of the above cited screening requirements.

A Permitted Individual's access to CJI may be terminated with or without cause at the discretion of the Superintendent, CJI Officer, or their respective designees. Upon termination of the Permitted Individual's employment in or contract with the District, such individual's access to CJI is to be immediately terminated. Reassignment or modification of a Permitted Individual's professional responsibilities is considered cause to reconsider CJI access.

Maintenance and Safeguarding of Criminal Justice Information (CJI)

The District will designate the locations, files and information systems where CJI is to be maintained. These controlled areas, locked when unattended, are limited to Permitted Individuals and other authorized personnel. If not possible to reasonably restrict access, all CJI is to be maintained in encrypted format in a manner consistent with legal requirements and industry standards.

The written approval of the CJI Officer is required in order to remove CJI from a controlled area. The CJI Officer must develop a protocol to ensure the protection of CJI while being transported and while out of the controlled area.

Maintenance and Safeguarding of Criminal Justice information (CJI) (continued)

CJI that is maintained in paper format must be kept in a physically secure location, with a posted notice of restricted access to such records. An access log or sign-in sheet is to be used to record access to paper records.

The Criminal Justice Information Services (CJIS) Security Policy contains safeguards for CJI records maintained in electronic format which the District shall comply. These safeguards include, but are not limited to, maintaining CJI on secure electronic systems and media; positioning information systems in a manner to prevent unauthorized individuals access and viewing CJI; storing electronic media containing CJI in a secure location; instituting access controls to limit access to Permitted Individuals; validating and authenticating information system users accessing CJI; developing protocols for configuration management and providing necessary access for system modifications and maintenance; providing the capability to detect and protect against threats to the integrity of CJI; developing parameters for auditing electronic systems containing CJI; and instituting media protection policies and procedures.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Disclosure of CJI by Permitted Individuals

CJI may be disclosed by Permitted Individuals to (1) District staff upon written approval of the Superintendent, CJI Officer or their respective designees when such disclosure is viewed as reasonably necessary for the performance of District function or policy or consistent with applicable law; (2) third-party individuals/entities when such disclosure has been approved by the Superintendent or CJI Officer or their respective designees, when consistent with applicable law; or as otherwise required or permitted by law. All such disclosures shall be logged.

Security Incident Response

"Security Incident" is the actual or suspected acquisition, access, use, or disclosure of CJI in a manner not permitted by these regulations or applicable law. A Security Incident must be reported immediately to the CJI Officer, who will investigate, collect relevant evidence and respond to all such incidents.

The CJI Officer is to document each security incident including the District's response, steps taken to mitigate harm to the affected individuals and changes, as necessary to District policies and procedures to avoid a reoccurrence of such incidents.

Security incidents are to be reported in writing to the District, regarding an individual's CJI that may have been accessed, acquired or disclosed during the Security Incident. Affected individuals and/or appropriate government agencies will be notified by the District as required by law or as the District determines appropriate.

Record Retention, Disposal and Destruction of CJI

CJI shall be maintained by the District in conformity with applicable record retention laws. Records containing CJI shall be stored for extended periods only if they are key elements for the integrity and/or utility of case files and/or criminal record files. Any audit records and transaction logs are to be maintained for one year. All records containing CJI are to be destroyed when the District is no longer required to keep CJI on file.

CJI containing paper records shall be disposed of as to make them unreadable and unable to be reconstructed, by shredding or incineration of such records. Electronic media containing CJI shall be destroyed utilizing a method that renders the CJI unreadable, indecipherable or unable to be reconstructed. Media destruction is to be done only by authorized personnel and witnessed and the method used documented.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Training

District staff with access to CJI shall initially be trained in the use, disclosure and safeguarding of such information and no less than biennially after the initial training.

(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181, June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67)

17a-101k Registry of findings of abuse or neglect of children maintained by Commissioner of Children and Families. Notice of finding of abuse or neglect of child. Appeal of finding. Hearing procedure. Appeal after hearing. Confidentiality. Regulations.

29-17a Criminal history checks. Procedure. Fees.

PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records.

PA 16-83 An Act Concerning Fair Chance Employment

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

*****This section of the administrative regulation pertaining to Criminal Justice Information (CJI) is based upon information originally developed by the law firm of Shipman and Goodwin.

Regulation approved: November 7, 2017 NEWTOWN PUBLIC SCHOOLS
Regulation revised: November 9, 2017
Regulation revised: January 9, 2024 Newtown, Connecticut