Personnel -- Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

Criminal Justice Information

In order to create a safe and orderly environment for students, all offers of employment will be conditional upon the successful outcome of a criminal record check. In addition, any person applying for employment with the Board shall submit to a record check of the Department of Children and Families (DCF) Child Abuse and Neglect Registry before the person may be hired.

Note: *Applicants for all positions, certified or non-certified must submit to a check of Department of Children and Families Child Abuse and Neglect Registry.*

Applicants, as required, shall make disclosures containing (1) current and past employers' contact information; (2) authorization allowing contact with such employers; and (3) statements about any past misconduct, discipline, or licensure penalties as a result of sexual misconduct or abuse allegations.

The District, prior to hiring such applicants, applicants, will (1) ensure that they complete the above stated three requirements; (2) review applicants' employment history after making a documented, good faith effort to contact previous employers for information; and (3) request any available information about applicants from SDE.

The background/reference checks shall be done in compliance with the statutory guidelines contained in Board policy #4112.51/4212.51, as updated in 2019.

District employees shall within 30 days after they are hired submit to state and national criminal checks. District students employed by the school system are exempted from this requirement.

Workers placed in a school under a public assistance employment program shall also submit to the criminal check if such individuals will have direct contact with students.

Student teachers placed in District schools as part of completing preparation requirements for the issuance of an educator certificate shall also be required to undergo the same criminal background checks and DCF child abuse and neglect registry check already required for school employees.

A District student, employed by the District or a person employed by the Board as a teacher for a non-credit adult class or adult education activity (as defined in C.G.S. 10-67) who is not required to hold a teaching certificate, pursuant to C.G.S. 10-145b, as amended by PA 18-51, is exempt from the fingerprinting requirement.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information (continued)

Criminal Justice Information

Criminal Justice Information (CJI) is to be maintained in accordance with the administrative regulation pertaining to the use and disclosure of criminal justice information.

(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, PA 16-67, PA 18-51, and PA 19-91)

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.

Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, June 2019

Policy adopted: November 3, 2025

REGIONAL SCHOOL DISTRICT NO. 14
Bethlehem and Woodbury, Connecticut

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction

The following administrative regulations are developed to ensure Criminal Justice Information compliance:

Relevant Acronym Key

CJI/CJIS	**Criminal Justice Information/Services**
CJA	**Criminal Justice Agency**
CSA	**CJIS Systems Agencies**
CSO	**CJIS Systems Officer**
CGA	**Contracting Government Agency**
AC	**Agency Coordinator**
CSA ISO	**CJIS Systems Agency Information Security Officer**
LASO	**Local Agency Security Officer**
FBI CJIS ISO	**FBI CJIS Division Information Security Officer**
CJI	**Criminal Justice Information**
CHRI	**Criminal History Record Information**
PII	**Personally Identifiable Information**
COLLECT CJBAU	**C**T **O**n-**L**ine **L**aw **E**nforcement **C**ommunications **T**eleprocessing **C**riminal **J**ustice **B**usiness **A**pplications **U**nit

Purpose

This policy is applicable to any fingerprint-based state and national criminal history record check made for non-criminal justice purposes and requested under applicable federal authority and/or state statute authorizing such checks for hiring personnel for employment in the Region 14 School District.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. While the Region 14 School District may complement CJIS policy with local requirements, CJIS policy shall always be the minimum standard. The local policy may augment or increase the standards but shall not detract from the CJIS Security Policy Standards.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

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

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

Requesting CHRI Checks

Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and the Connecticut Department of Emergency Services and Public Protection – COLLECT CJBAU, in accordance with all applicable state and federal rules and regulations.

If an applicant or employee is required to submit to a fingerprint-based state and national criminal history record check, they shall be informed of this requirement and instructed on how to comply with the law. Such instructions will include information on the procedure for submitting fingerprints. In addition, the applicant or employee will be provided with all information needed to successfully register for a fingerprinting appointment.

Acceptable Use of CHRI

All CHRI is subject to strict state and federal rules and regulations. CHRI is used only for the official purpose for which it was requested, and CHRI cannot be shared with other entities for any purpose, including subsequent hiring determinations. All receiving entities are subject to audit by the COLLECT CJBAU (Connecticut On-Line Law Enforcement Communications Teleprocessing/Criminal Justice Business Applications Unit) and the FBI, and failure to comply with such rules and regulations could lead to sanctions. Furthermore, the Region 14 School District and the employee responsible for overseeing CJI can be charged with federal and state crimes for the willful, unauthorized disclosure of CHRI.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Personnel Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI for the Region 14 School District will review and become familiar with educational and relevant training materials regarding CHRI laws and regulations made available by the appropriate agencies.

In addition to the above, all personnel authorized to receive and/or review CHRI must undergo Security Awareness Training on a biennial basis. This training will be accomplished using the training provided by CJIS Online.

The Superintendent or his/her/their designee will be responsible for overseeing all training programs and adherence to all training requirements.

Personnel Security (All Personnel)

All personnel requiring access to CHRI must first be deemed "Authorized Personnel" by the Superintendent or his/her/their designee. The COLLECT CJBAU will review and determine if access is appropriate. Access is denied if the individual has ever had a felony conviction of any kind, no matter when it occurred. Access may be denied if the individual has one or more recent misdemeanor convictions.

In addition to the above, an individual believed to be a fugitive from justice or having an arrest history without convictions will be reviewed to determine if access to CHRI is appropriate. The COLLECT CJBAU will take into consideration extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

Persons already having access to CHRI and who are subsequently arrested and/or convicted of a crime will:

1. Have their access to CVHRI suspended until the outcome of an arrest is determined and reviewed by the COLLECT CJBAU to determine if continued access is appropriate;
2. Have their access suspended indefinitely if a conviction results in a felony of any kind;
3. Have their access denied by the COLLECT CJBAU, where it is determined that access to CHRI by the person would not be in the public's best interest.

Support personnel, contractors, and custodial workers will be denied access to CHRI. If such persons need to be in an area (s) where CHRI is maintained or processed (at rest or in transit), they will be escorted by authorized personnel or under their supervision at all times while in the area(s).
.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Personnel Termination

The Local Agency Security Officer (LASO) shall terminate access to CHRI immediately upon notification of an individual's termination of employment.

The Region 14 School District shall follow the following CHRI termination process:

1. Notification will be sent via email to the COLLECT CJBAU;
2. This is to be done within 24 hours of receiving notification of termination;
3. All keys, email accounts, and other district accounts and materials identified by the Superintendent. will be obtained/disabled from the user within 24 hours.

Adverse Decisions Based on CHRI

If inclined to make an adverse decision based on an individual's CHRI, the Region 14 School District will take the following steps prior to making a final adverse determination:

1. Provide the individual the opportunity to complete or challenge the accuracy of his/her/their CHRI; and
2. Provide the individual with information on the process for updating, changing, or correcting CHRI.

A final adverse decision based on an individual's CHRI will not be made until the individual has been afforded a reasonable fifteen-day period (15) to correct or complete the CHRI.

Non-Criminal Agency Coordinator (TAC)

The Region 14 School District TAC is the Director of Finance and Operations and is responsible for the following:

1. Maintaining an updated Authorized Personnel List on file with the COLLECT CJBAU.
    a. Ensuring everyone included on this list must undergo the appropriate level of CJIS Security Awareness Training;
    b. Ensuring everyone included on the list has appropriate access based on job functions and a need-to-know basis.
2. Inform the COLLECT CJBAU of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.).
    a. Contact the COLLECT CJBAU immediately to update the User Agreement and, if necessary, submit the new authorization to the COLLECT CJBAU;
    b. Submit a TAC change form to the COLLECT CJBAU in the event of a change in roles.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Local Agency Security Officer (LASO)

The Region 14 School District LASO is the Director of Finance and Operations and is responsible for the following:

1. Identifying who is using or accessing CHRI and/or systems with access to CHRI;
2. Ensuring that personnel security screening procedures are being followed as stated in this policy.
3. Ensuring the approved and appropriate security measures are in place and working as expected.

Storage of CHRI

CHRI shall only be stored for extended periods of time when necessary to ensure the integrity and/or utility of an individual's personnel file. Administrative, technical, and physical safeguards, which comply with the most recent COLLECT CJBAU and FBI Security Policy, have been implemented to ensure the security and confidentiality of CHRI. Each individual involved in the handling of CHRI is to become familiarized with these safeguards.

In addition to the above, each individual involved in handling CHRI will strictly adhere to the policy on its storage and destruction.

Media/Physical Protection

All media containing CHRI must be protected and secured at all times. The following is established and to be implemented to ensure the appropriate security, handling, transporting, and storage of CHRI media in all forms.

Controls shall be in place to protect electronic and physical media containing CHRI 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 CHRI.

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

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Physical Storage and Access

Physical CHRI media shall be securely stored within physically secured locations or controlled areas. A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient 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. Access to such media is restricted to authorized personnel only and shall be secured at all times when not in use or under the supervision of an authorized individual.

Only authorized personnel will have access to physically secure non-public locations. The Superintendent or his/her/their designee will maintain and keep a list of authorized personnel. Before granting access, all physical access points into the District's secure areas will be authorized. The Superintendent or his/her/their designee 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 agency from physical, logical, and electronic breaches.

Physical CHRI media:

1. Is to be stored within employee records when feasible or by itself when necessary.
2. Is to be maintained within a lockable filing cabinet, drawer, closet, office, safe, vault, or other secure container.

Electronic CHRI media:

1. Is to be stored on secure servers within a physically secure location when feasible.
2. (Include details on how electronic CHRI is secured.)

Destruction of CHRI

Disposal of Physical Media

Once physical CHRI media (paper/hard copies) is determined to be no longer needed by the District, it shall be destroyed and disposed of appropriately. Physical CHRI media shall be destroyed by cross-cut shredding or incineration. The Superintendent or his/her/their designee will ensure such destruction is witnessed or carried out by authorized personnel:

1. The LASO shall witness or conduct disposal
2. Cross-cut shredding will be the method of destruction used by the District.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Destruction of CHRI

Media Sanitization and Disposal (Disposal of Electronic Media)
Once the District determines that electronic CHRI media (data stored on computers) are no longer needed, they shall be destroyed and disposed of appropriately.

The Region 14 Public Schools shall choose one of the following options below to use in this policy:

Option 1: Overwriting

Overwriting involves a program writing onto the media where the file to be sanitized is located. The NCJA will sanitize the electronic CHRI by overwriting the data at least three times before disposing of or reusing the computer/device/system on which it was stored. Overwriting the CHRI data must be completed or witnessed by authorized district personnel.

Option 2: Degaussing

Degaussing is a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets are weak and cannot effectively degauss magnetic media. The NCJA will degauss the electronic CHRI prior to disposing of or reusing the computer/device/system on which the electronic CHRI was stored. Degaussing the CHRI data must be completed or witnessed by authorized district personnel. (Degaussing means neutralizing a magnetic field to erase information from a magnetic disk or other storage device.)

Option 3: Destruction

If the computer/device on which the CHRI data is stored is no longer operational, The NCJA must physically destroy the device. Destruction of the device containing physical electronic CHRI, including printouts and other media, shall be disposed of by one of the following methods:

Remote Access

The Superintendent 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 means any temporary access to an agency's information system by a user or information system communicating temporarily through an external, non-district-controlled network, such as the Internet.

The District shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The Superintendent or his/her/their designee shall control all remote access through managed access control points and may permit remote access for privileged functions only for compelling operational needs. However, this person shall document the rationale for such access in the security plan for the information system.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction

Destruction of CHRI (continued)

Remote Access (continued)

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

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes portable technology like a camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards, mobile wireless devices, or any personal desktop computer. When bringing your own devices are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

Disciplinary

If an individual employed by the Region 14 Public School District has misused or is currently misusing CHRI, the following requirements will be adhered to:

1. Using CHRI for any purpose other than what is allowed by state statute or Federal code is considered misuse.
2. **The specific steps the District will take in the event intentional misuse is discovered.
3. Misuse of CHRI can result in loss of access to CHRI, loss of employment, and/or criminal prosecution.
4. Misuse of CHRI shall be reported to the State.

Incident Response

The security of information and systems in general, and of CHRI in particular, is a top priority for the Region 14 Public School district. Therefore, the District has established appropriate operational incident response procedures for instances of an information security breach. It is each individual's responsibility to adhere to established security guidelines and policies and to be attentive to situations and incidents that pose risks to security. Furthermore, it is each individual's responsibility to immediately report potential or actual security incidents to minimize any breach of security or loss of information.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction

Incident Response (continued)

The following security incident handling procedures must be followed by each individual:

1. All incidents will be reported directly to the LASO.
2. If any records are stolen, the incident will also be reported to appropriate authorities.
3. Once the cause of the breach has been determined, disciplinary measures will be taken in accordance with the disciplinary policy of the District

In addition to the above, the LASO shall report all security-related incidents to the COLLECT CJBAU within 24 hours.

All District personnel with access to FBI and/or COLLECT CJBAU CHRI have a duty to protect the system and related systems from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the information. All existing laws, District regulations, and policies apply, including those that may apply to personal conduct. Misuse or failure to secure any information resources may result in temporary or permanent restriction of all privileges up to employment termination.

The Superintendent shall ensure that all staff members are aware of this policy and that those responsible for implementation and oversight receive adequate training and updates.

(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, PA 16-67 and PA 18-51, and PA 19-91)
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 Plan, Version 5.8, 06/01/2019 Prepared by CJIS Information Officer Approved by CJIS Advisory Policy Board

Regulation approved: November 3, 2025

REGIONAL SCHOOL DISTRICT NO. 14
Bethlehem and Woodbury, Connecticut