

Suggested replacement for existing policy, presently numbered 4112.51/4212.5 adopted 11/19/12 which does not reflect legislative modifications.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

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 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 amended.

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.

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.

Student teachers placed in District schools as part of completing preparation requirements for the issuance of an educator certificate, effective July 1, 2010, shall also be required to undergo the same criminal background checks already required for school employees.

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. 10-14Sb, as amended by PA 18-51, is exempt from the fingerprinting requirement.

Personnel-- Certified/Non-Certified

Security Check/Fingerprinting (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 and PA 18-51)

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.

Policy adopted:

Agency Privacy Requirements for Noncriminal Justice Applicants

Authorized governmental and non-governmental agencies/officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice purpose (such as a job or license, immigration or naturalization matter, security clearance, or adoption) are obligated to ensure the applicant is provided certain notice and other information and that the results of the check are handled in a manner that protects the applicant's privacy.

- Officials must provide to the applicant written notice (*Written notice includes electronic notification, but excludes oral notification*) that his/her fingerprints will be used to check the criminal history records of the FBI.
- Officials using the FBI criminal history record (if one exists) to make a determination of the applicant's suitability for the job, license, or other benefit must provide the applicant the opportunity to complete or challenge the accuracy of the information in the record.
- Officials must advise the applicant that procedures for obtaining a change, correction, or updating of an FBI criminal history record are set forth at Title 28, Code of Federal Regulations (CFR), Section 16.34.
- Officials should not deny the job, license, or other benefit based on information in the criminal history record until the applicant has been afforded a reasonable time to correct or complete the record or has declined to do so.
- Officials must use the criminal history record solely for the purpose requested and cannot disseminate the record outside the receiving department, related agency, or other authorized entity. (See 5 U.S.C. 552a(b); 28U.S.C. 534(b); 42 U.S.C. 14616, Article IV(c); 28 CFR 20.21(c), 20.33(d), 50.12(b) and 906.2(d))

The FBI has no objection to officials providing a copy of the applicant's FBI criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant the time and additional FBI fee to obtain his/her record directly from the FBI by following the procedures found at 28 CFR 16.30 through 16.34. It will also allow the officials to make a more timely determination of the applicant's suitability.

Each agency should establish and document the process/procedures it utilizes for how/when it gives the applicant notice, what constitutes "a reasonable time" for the applicant to correct or complete the record, and any applicant appeal process that is afforded the applicant. Such documentation will assist State and/or FBI auditors during periodic compliance reviews on use of criminal history records for noncriminal justice purposes.

Connecticut Records:

Department of Emergency Services and Public Protection
State Police Bureau of Identification (SPBI)
111 Country Club Road
Middletown, CT 06457
860-685-8480

Out-of-State Records:

Agency of Record
OR
FBI CJIS Division-Summary Request
1000Custer Hollow Road
Clarksburg, West Virginia 26306

If you need additional information or assistance, contact:_____

Noncriminal Justice Applicant's Privacy Rights

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for a job or license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below.

- You must be provided written notification by _____ that your fingerprints will be used to check the criminal history records of the FBI.
- If you have a criminal history record, the officials making a determination of your suitability for the job, license, or other benefit must provide you the opportunity to complete or challenge the accuracy of the information in the record.
- The officials must advise you that the procedures for obtaining a change, correction, or updating of your criminal history record are set forth at Title 28, Code of Federal Regulations (CFR), Section 16.34.
- If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the job, license, or other benefit based on information in the criminal history record (See 28 CFR 50.12(b)).
- You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council. (See 5 U.S.C. 552a(b); 28U.S.C. 534(b); 42 U.S.C. 14616, Article IV(c); 28 CFR 20.21(c), 20.33(d), 50.12(b) and 906.2(d)).
- If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at <http://www.fbi.gov/about-us/cjis/background-checks>.
- If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI at the same address as provided above. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)

Connecticut Records:

Department of Emergency Services and Public Protection
State Police Bureau of Identification (SPBI)
111 Country Club Road
Middletown, CT 06457
860-685-8480

Out-of-State Records:

Agency of Record
OR
FBI CJIS Division-Summary
Request IOOCuster Hollow Road
Clarksburg, West Virginia 26306

If you need additional information or assistance, please contact: _____

**Federal Bureau of Investigation
United States Department of
Justice Privacy Act Statement**

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Social Security Account Number (SSAN). Your SSAN is needed to keep records accurate because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 USC 552a), the requesting agency is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other authority your SSAN is solicited, and what uses will be made of it. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

Additional Information: The requesting agency and/or the agency conducting the application-investigation will provide you additional information pertinent to the specific circumstances of this application, which may include identification of other authorities, purposes, uses, and consequences of not providing requested information. In addition, any such agency in the Federal Executive Branch has also published notice in the Federal Register describing any systems(s) of records in which that agency may also maintain your records, including the authorities, purposes and routine uses for the system(s).



STATE OF CONNECTICUT

DEPARTMENT OF EMERGENCY SERVICES AND PUBLIC PROTECTION

Automated Fingerprint Identification System (AFIS) Agreement for Fingerprint Card Submissions

by and between

the State of Connecticut Department of Emergency Services and Public Protection
and

Woodbridge Public School, Board of Education

WHEREAS, the State of Connecticut Department of Emergency Services and Public Protection (hereinafter "DESPP") operates a central Automated Fingerprint Identification System (hereinafter "AFIS"); and

WHEREAS, Woodbridge Public School, Board of Education (hereinafter "BOE"), is established pursuant to Connecticut General Statutes (C.G.S.) § 10-220 and has been authorized to submit hard copy fingerprint cards to AFIS pursuant to the limited purposes set forth in C.G.S. § 10-212, § 10-221d, the Adam Walsh Act of 2006 (AWA), and the National Child Protection Act 1993/Nolunteers for Children Act of 1998 (NCPANCA), as applicable.

WHEREAS, the BOE is a qualified entity pursuant to the NCPAN CA.

NOW, THEREFORE, DESPP and BOE, by and through their Commissioners or other authorized individuals, enter into this Agreement to permit BOE to send hard copy fingerprint cards to the State Police Bureau of Identification (SPBI) for submission to AFIS and receive back the results of the state and/or national criminal history record information (CHRI) via email.

- 1. Effective Date.** This Agreement shall be effective upon signature by both parties.
- 2. Authority to Enter Agreement.** DESPP is authorized to enter into this agreement through the Commissioner of the Department of Emergency Services and Public Protection, pursuant to the authority provided under C.G.S. § 4-8.
- 3. Duration of Agreement.** This Agreement shall remain in full force and effect unless terminated by DESPP, giving BOE written notice of such intention at least thirty (30) days in advance. DESPP reserves the right to suspend or revoke access to CHRI without notice in the event of a breach of the conditions of this Agreement. Notwithstanding any provisions in this Agreement, DESPP, through a duly authorized employee, may terminate the Agreement whenever DESPP makes a written determination that such termination is in the best interests of the State. DESPP shall notify BOE in writing of termination pursuant to this section, which notice shall specify the effective date of termination and the extent to which BOE must complete its performance under the Agreement prior to such date.

4. DESPP Responsibilities. DESPP shall:

- a) Electronically process BOE applicant prints as required and report results of required state and/or national record checks via a generic email.
- b) Identify a liaison as the primary point of contact for any issues related to this agreement.

5. BOE Responsibilities. BOE shall:

- a) Provide qualifying fingerprints that meet submission criteria pursuant to the specific purposes pursuant to C.G.S. §10-212, §10-221d, the AWA, and/or the NCPA/VCA.
- b) Assign a Local Agency Security Officer (hereinafter "LASO") in accordance with the United States Department of Justice (USDOJ) FBI Criminal Justice Information Services Security Policy (hereinafter "CJIS Security Policy").
- c) Ensure appropriate security measures as applicable to the physical security of communication equipment; personnel security to include screening requirements; technical security to protect against unauthorized use; and security of criminal justice information (hereinafter "CJI") in accordance with the provisions of the CJIS Security Policy. BOE shall further:
 - a. Assign a generic email to be used by DESPP to communicate CJI, CHRI and related notifications only.
 - b. Ensure that CJI is maintained in a physically secure location or controlled area as defined in the CJIS Security Policy.
 - c. Ensure that all persons with access to physically secure locations or controlled areas, including, but not limited to, support personnel, contractors, vendors, and custodial workers, are escorted by authorized personnel at all times. Authorized personnel are BOE personnel who have been appropriately trained and vetted through the screening process and have been granted access to CJI for the specific purposes provided in the C.G.S. §10-212, §10-221d, the AWA, and/or the NCPA/VCA. The use of cameras or other electronic means to monitor a physically secure location or controlled area does not constitute an escort.
 - d. Ensure that access to CJI, in any form, is limited to BOE personnel requiring access to such information for the specific purposes provided in the C.G.S. §10-212, §10-221d, the AWA, and/or the NCPA/VCA.
 - e. Ensure that all BOE personnel accessing CJI are properly trained before access to CJI is authorized. Training must include Security Awareness Training in accordance with the provisions of the CJIS Security Policy.
 - f. Ensure that BOE personnel having access to CJI sign an acknowledgment form attached hereto as Attachment A acknowledging that they have received copies of this Agreement and Attachment A and that they are responsible for complying with the terms contained therein. Such forms shall be maintained in the official personnel files of such personnel.
- d) Ensure that all security incidents are reported to the CJIS Security Officer ("CSO") or their designee. If a person already has access to CJI and is subsequently arrested and/or convicted, continued access to CJI shall be determined by the CSO. If the CSO or their designee determines that access to CJI by the person would not be in the public interest, access shall be denied and BOE shall be notified in writing of the access denial.

- e) Comply with all audit requirements for CJIS Systems, including, but not limited to, appropriate and reasonable quality assurance procedures.
- f) Ensure that, prior to fingerprinting, all persons fingerprinted are provided with a copy of the Noncriminal Justice Applicant's Privacy Rights form.
- g) Ensure that, prior to fingerprinting, all persons fingerprinted pursuant to NCPA/VCA are provided with a NCPA/VCA Waiver and Consent Form (Waiver). A copy of the Waiver shall be maintained for a minimum of one year from the date of fingerprint submission.
- h) Violations of the CJIS Security Policy can result in the suspension or termination of system access for BOE, individual suspension or termination of access to CJI, criminal and/or administrative investigation, arrest, and/or prosecution and conviction for violation of state and federal statutes designated to protect confidentiality and integrity of CJI and related data.

6. **Transaction Fees.** BOE applicants shall remit full payment for all transactions with the submission of hard copy fingerprint cards.

The fingerprinting fee at a Connecticut State Police location shall be fifteen (\$15.00) dollars, and the fingerprinting fee varies if fingerprints are taken by a local police location. Fees are subject to change due to legislative enactments and federal assessments.

7. **Modification or Amendment of the Agreement.** This Agreement may not be modified or amended unless in writing signed by an authorized representative of both parties.

8. Indemnification

BOE shall indemnify and hold harmless the State of Connecticut, the State of Connecticut Department of Emergency Services and Public Protection, its officers, agents, employees, commissions, boards, departments, divisions, successors and assigns from and against all actions (pending or threatened and whether at law or in equity in any forum), liabilities, damages, losses, costs and expenses, including but not limited to reasonable attorneys' and other professionals' fees, resulting from (i) misconduct or negligent or wrongful acts (whether of commission or omission) of BOE or any of its officers, representatives, agents, servants, consultants, employees or other persons or entities with whom BOE is in privity of oral or written contract; (ii) liabilities arising directly or indirectly in connection with this Agreement out of the acts of BOE and (iii) damages, losses, costs and expenses, including but not limited to, attorneys' and other professionals' fees, that may arise out of such claims and/or liabilities.

9. The following documents are incorporated by reference and made part of this MOU:
- a. CJIS Security Policy;
 - b. National Crime Prevention and Privacy Compact, 42 U.S.C. Section 14616; and
 - c. Title 28, Code of Federal Regulations, Parts 20 and 25, Section 50.12, and Chapter IX.

THE DEPARTMENT OF EMERGENCY SERVICES AND PUBLIC PROTECTION

By: _____ (Date)
Dora B. Schriro
Commissioner
Duly Authorized Pursuant to C.G.S. Section 4-8

BOE

By: _____ (Date)
Name
Title
Duly Authorized

ATTACHMENT A

ACKNOWLEDGEMENT

I, _____ acknowledge the following:

1. I have received a copy of the Agreement between the State of Connecticut Department of Emergency Services and Public Protection ("DESPP") and the BOE concerning access to the DESPP Automated Fingerprint Identification System ("AFIS").
2. I understand that I am being allowed to submit applicant prints via hard copy fingerprint cards into AFIS pursuant to a Federal Bureau of Investigation-approved state or federal statute.
3. I understand that I am not authorized to submit any other fingerprints into AFIS except those authorized by the Agreement.
4. I will fully cooperate with state or federal personnel regarding any audit, system check, and user privilege inquiries.
5. I understand that I am responsible for complying with the Agreement between the State of Connecticut DESPP and the BOE and that noncompliance may result in suspension or revocation of user privileges and/or other action as provided by law.

By: _____
Signature Date

cc: Official Personnel File

~~Existing policy which does not have an adoption date. Remove this from the manual. It duplicates, with exact same language, the District's existing #4112.5/4212.5.~~

~~Personnel-Certified~~

~~Security Check/Fingerprinting~~

~~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. District employees shall submit to state and national criminal checks within 30 days of hire. Failure to comply will result in termination.~~

~~Legal Reference: Connecticut General Statutes
10-221d Criminal History Records Check of School Personnel.
Fingerprinting Termination of Dismissed. (as amended by PA 01-173)~~

Policy adopted:

WOODBRIIDGE PUBLIC SCHOOLS
Woodbridge, Connecticut