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. An applicant has an affirmative duty to consent to such identification as may be necessary to allow a criminal record check to be conducted. 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 positions requiring a state certificate, authorization or permit must submit to a check of DCF's abuse and neglect registry, effective. Applicants for positions not requiring state certification are required to submit to the DCF 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, 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, shall also be required to undergo the same criminal background checks already required for school employees.

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.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

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, Public Act No. 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.

Policy adopted: August 24, 2000
Policy revised: February 28, 2002
Policy revised: November 18, 2004
Policy revised: April 29, 2010
Policy revised: May 24, 2012
Policy revised: January 26, 2017
Policy revised: June 22, 2017

MARLBOROUGH PUBLIC SCHOOLS
Marlborough, 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 by the Regional Service Center. This packet shall also contain all documents and materials necessary for the Regional Service Center 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 in writing 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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

   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:

      i. 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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

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. Applicants for substitute teaching positions must also fulfill the disclosure requirements as listed above. The District will also request information from the applicant's prior employers and SDE (in the same manner required for other applicants).

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

12. Adult education teachers and substitute teachers, if they are continuously employed by the district, do not have to be refingerprinted after fulfilling the initial requirement.

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 are required to be fingerprinted at one of the RESCs and not 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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

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.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

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.

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

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Legal Reference: Connecticut General Statutes (continued)

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.

Regulation approved: June 22, 2017

MARLBOROUGH PUBLIC SCHOOLS
Marlborough, Connecticut

4112.5/4212.5
Appendix A

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: Marlborough School District.

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 the Marlborough School District 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 CFR16.30 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
1000Custer Hollow Road
Clarksburg, West Virginia 26306

If you need additional information or assistance, please contact: Marlborough School District.

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 Marlborough 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, **Marlborough 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/Volunteers for Children Act of 1998 (NCPA/VCA), as applicable.

WHEREAS, the BOE is a qualified entity pursuant to the NCPA/VCA.

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. Fees shall be calculated as follows:

Statute	Category	State Fee	Federal Fee
C.G.S. §10-212	BOE Nurse or Nurse Practitioner	$0.00	$12.00
C.G.S. §10-221d	BOE Employee	$0.00	$12.00
AWA	Individual employed, under consideration for employment, or otherwise in a position in which the individual would work with or around children in the school.	$50.00	$12.00
AWA Volunteer	Volunteers in a position in which the individual would work with or around children in the school.	$50.00	$10.75
NCPA/VCA	Individuals who provide treatment, education, training, instruction, supervision, or recreation to children, the elderly, or individuals with disabilities on behalf of the BOE.	$50.00	$12.00
NCPA/VCA Volunteer	Volunteers who provide treatment, education, training, instruction, supervision, or recreation to children, the elderly, or individuals with disabilities on behalf of the BOE.	$50.00	$10.75

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

BOE

By: _____ _____
Name (Date)
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