Series 4000
Personnel
4112.2

EMPLOYMENT CHECKS

As set forth below, each applicant for a position with the district shall be asked whether he/she has ever been convicted of a crime, whether there are any criminal charges pending against him/her and whether the applicant is included on the Abuse and Neglect Registry of the Connecticut Department of Children and Families ("DCF") (the "Registry"). Applicants shall not be required to disclose any arrest, criminal charge or conviction that has been erased.

In addition, the district shall conduct an employment history check for each applicant for a position, as set forth below.

For the purposes of this policy:

"Sexual misconduct means" any verbal, nonverbal, written, or electronic communication, or any other act directed toward or with a student that is designed to establish a sexual relationship with the student, including a sexual invitation, dating or soliciting a date, engaging in sexual dialog, making sexually suggestive comments, self-disclosure or physical exposure of a sexual or erotic nature, and any other sexual, indecent, or erotic contact with a student.

"Abuse or neglect" means abuse or neglect as described in Conn. Gen. Stat. § 46b-120, and includes any violation of Conn. Gen. Stat. §§ 53a-70 (sexual assault in the first degree), 53a-70a (aggravated sexual assault in the first degree), 53a-71 (sexual assault in the second degree), 53a-72a (sexual assault in the third degree), 53a-72b (sexual assault in the third degree with a firearm), or 53a-73a (sexual assault in the fourth degree).

"Former employer" means any person, firm, business, educational institution, nonprofit agency, corporation, limited liability company, the state, any political subdivision of the state, any governmental agency, or any other entity that such applicant was employed by <u>during any of the previous twenty years</u> prior to applying for a position with a local or regional board of education.

I. <u>Employment History Check Procedures</u>

A. The district shall not offer employment to an applicant for a position, including any position that is contracted for, if such applicant would have direct student contact, prior to the district:

1. Requiring the applicant:

a. to list the name, address, and telephone number of each current employer or former employer (please note the definition of "former employer" employer above, including the applicable twenty year reporting period) during any of the previous twenty years), if:

(i) such current or former employer is/was a local or regional board of education, council of a state or local charter school, interdistrict magnet school operator, or a supervisory agent of a nonpublic school, and/or

(ii) the applicant's employment with such current or former employer caused the applicant to have contact with children.

b. to submit a written authorization that

(i) consents to and authorizes disclosure by the employers listed under paragraph I.A.1.a of this policy of the information requested under paragraph I.A.2 of this policy and the release of related records by such employers,

(ii) consents to and authorizes disclosure by the Department of Education of the information requested under paragraph I.A.3 of this policy and the release of related records by the department, and

(iii) releases those employers and the Department of Education from liability that may arise from such disclosure or release of records pursuant to paragraphs I.A.2 or I.A.3 of this policy; and

c. to submit a written statement of whether the applicant

(i) has been 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) has ever been disciplined or asked to resign from employment or resigned from or otherwise separated from any employment while an allegation of abuse or neglect was pending or under investigation by DCF, or an allegation of sexual misconduct was pending or under investigation or due to an allegation substantiated pursuant to Conn. Gen. Stat. § 17a-101g or abuse or neglect, or of sexual misconduct or a conviction for abuse or neglect or sexual misconduct, or

(iii) has ever had a professional or occupational license or certificate suspended or revoked or has ever surrendered such a license or certificate 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 due to an allegation substantiated by DCF of abuse or neglect or of sexual misconduct or a conviction for abuse or neglect or sexual misconduct;

2. Conducting a review of the employment history of the applicant by contacting those employers listed by the applicant under paragraph I.A.1.a of this policy. Such review shall be conducted using a form developed by the Department of Education, which shall request the following:

a. the dates employment of the applicant, and

b. a statement as to whether the employer has knowledge that the applicant:

(i) was the subject of an allegation of abuse or neglect or sexual misconduct for which there is an investigation pending with any employer, state agency, or municipal police department or which has been substantiated;

(ii) was disciplined or asked to resign from employment or resigned from or otherwise separated from any employment while an allegation of abuse or neglect or sexual misconduct was pending or under investigation, or due to a substantiation of abuse or neglect or sexual misconduct; or

(iii) has ever had a professional or occupational license, certificate, authorization or permit suspended or revoked or has ever surrendered such a license, certificate, authorization or permit while an allegation of abuse or neglect or sexual misconduct was pending or under investigation, or due to a substantiation of abuse or neglect or sexual misconduct. Such review may be conducted telephonically or through written communication. Notwithstanding the provisions of subsection (f) of Conn. Gen. Stat. § 31-51i, not later than five (5) business days after the district receives a request for such information about an employee or former employee, the district shall respond with such information. The district may request more information concerning any response made by a current or former employer for information about an applicant, and, notwithstanding subsection (f), such employer shall respond not later than five (5) business days after receiving such request.

3. Requesting information from the Department of Education concerning:

a. the eligibility status for employment of any applicant for a position requiring a certificate, authorization or permit,

b. whether the Department of Education has knowledge that a finding has been substantiated by DCF pursuant to Conn. Gen. Stat. § 17a-101g of abuse or neglect or of sexual misconduct against the applicant and any information concerning such a finding, and

c. whether the Department of Education has received notification that the applicant has been convicted of a crime or of criminal charges pending against the applicant and any information concerning such charges.

B. Notwithstanding the provisions of subsection (f) of Conn. Gen. Stat. § 31-51i, if the district receives information that an applicant for a position with or an employee of the board has been disciplined for a finding of abuse or neglect or sexual misconduct, it shall notify the Department of Education of such information.

C. The district shall not employ an applicant for a position involving direct student contact who does not comply with the provisions of paragraph I.A.1 of this policy.

D. The district may employ or contract with an applicant on a temporary basis for a period not to exceed ninety (90) calendar days, pending the district's review of information received under this section, provided:

1. The applicant complied with paragraph I.A.1 of this policy;

2. The district has no knowledge of information pertaining to the applicant that would disqualify the applicant from employment with the district; and

3. The applicant affirms that the applicant is not disqualified from employment with the district.

E. The district shall not enter into a collective bargaining agreement, an employment contract, an agreement for resignation or termination, a severance agreement, or any other contract or agreement or take any action that:

1. Has the effect of suppressing information relating to an investigation of a report of suspected abuse or neglect or sexual misconduct by a current or former employee;

2. Affects the ability of the district to report suspected abuse or neglect or sexual misconduct to appropriate authorities; or

3. Requires the district to expunge information about an allegation or a finding of suspected abuse or neglect or sexual misconduct from any documents maintained by the district, unless, after investigation, such allegation is dismissed or found to be false.

F. The district shall not offer employment to a person as a substitute teacher, unless such person and the district comply with the provisions of paragraph I.A.1 of this policy. The district shall determine which such persons are employable as substitute teachers and maintain a list of such persons. The district shall not hire any person as a substitute teacher who is not on such list. Such person shall remain on such list as long as such person is continuously employed by the district as a substitute teacher as described in paragraph III.B.2 of this policy, provided the district does not have any knowledge of a reason that such person should be removed from such list.

G. In the case of an applicant who is a contractor, the contractor shall require any employee with such contractor who would be in a position involving direct student contact to supply to such contractor all the information required of an applicant under paragraphs I.A.1.a and I.A.1.c of this policy and a written authorization under paragraph I.A.1.b of this policy. Such contractor shall contact any current or former employer (please note the definition of "former employer" employer above, including the applicable twenty year reporting period) of such employee that was a local or regional board of education, council of a state or local charter school, interdistrict magnet school operator, or a supervisory agent of a nonpublic school, or if the employee's employment with such current or former employer caused the employee to have contact with

children, and request, either telephonically or through written communication, any information concerning whether there was a finding of abuse or neglect or sexual misconduct against such employee. Notwithstanding the provisions of subsection (f) of Conn. Gen. Stat. § 31-51i, such employer shall report to the contractor any such finding, either telephonically or through written communication. If the contractor receives any information indicating such a finding or otherwise receives any information indicating such a finding or otherwise has knowledge of such a finding, the contractor shall, notwithstanding the provisions of subsection (f) of Conn. Gen. Stat. § 31-51i, immediately forward such information to the district, either telephonically or through written communication. If the district receives such information, it shall determine whether such employee may work in a position involving direct student contact at any school in the district. No determination by the district that any such employee shall not work under any such contract in any such position shall constitute a breach of such contract.

H. Any applicant who knowingly provides false information or knowingly fails to disclose information required in subdivision (1) of subsection (A) of this section shall be subject to discipline by the district that may include

1. denial of employment, or

2. termination of the contract of a certified employee, in accordance with the provisions of Conn. Gen. Stat. § 10-151.

I. If the district provides information in accordance with paragraph I.A.2 or I.G of this policy, the district shall be immune from criminal and civil liability, provided the district did not knowingly supply false information.

J. Notwithstanding the provisions of Conn. Gen. Stat. § 10-151c and subsection (f) of Conn. Gen. Stat. § 31-51i, the district shall provide, upon request by another local or regional board of education, governing council of a state or local charter school, interdistrict magnet school operator, or supervisory agent of a nonpublic school for the purposes of an inquiry pursuant to paragraphs I.A.2 or I.G of this policy or to the Commissioner of Education pursuant to paragraph I.B of this policy any information that the district has concerning a finding of abuse or neglect or sexual misconduct by a subject of any such inquiry.

K. Prior to offering employment to an applicant, the district shall make a documented good faith effort to contact each current and any former employer (please note the definition of "former employer" employer above, including the applicable twenty year reporting period) of the applicant that was a local or regional board of education, governing council of a state or local charter school, interdistrict magnet school operator, or supervisory agent of a nonpublic school, or if the applicant's employment with such current or former employer caused the applicant to have contact with children in order to obtain information and recommendations that may be relevant to the applicant's fitness for employment. Such effort, however, shall not be construed to require more than three telephonic requests made on three separate days.

L. The district shall not offer employment to any applicant who had any previous employment contract terminated by a local or regional board of education, council of a state or local charter school, interdistrict magnet school operator, or a supervisory agent of a nonpublic school, or who

resigned from such employment, if the person has been convicted of a violation of Conn. Gen. Stat. § 17a-101a, when an allegation of abuse or neglect or sexual assault has been substantiated.

II. DCF Registry Checks

Prior to hiring any person for a position with the district, the district shall require such applicant to submit to a records check of information maintained on the Registry concerning the applicant.

The district shall request information from the Registry or its out of state equivalent promptly, and in any case no later than thirty (30) calendar days from the date of employment. Registry checks will be processed according to the following procedure:

A. No later than ten (10) calendar days after the Superintendent or his/her designee has notified a job applicant of a decision to offer employment to the applicant, or as soon thereafter as practicable, the Superintendent or designee will either obtain the information from the Registry or, if the applicant's consent is required to access the information, will supply the applicant with the release form utilized by DCF, or its out of state equivalent when available, for obtaining information from the Registry.

B. If consent is required to access the Registry, no later than ten (10) calendar days after the Superintendent or his/her designee has provided the successful job applicant with the form, the applicant must submit the signed form to DCF or its out of state equivalent, with a copy to the Superintendent or his/her designee. Failure of the applicant to submit the signed form to DCF or its out of state equivalent within such ten-day period, without good cause, will be grounds for the withdrawal of the offer of employment.

C. Upon receipt of Registry or out-of-state registry information indicating previously undisclosed information concerning abuse or neglect investigations concerning the successful job applicant/employee, the Superintendent or his/her designee will notify the affected applicant/employee in writing of the results of the Registry check and will provide an opportunity for the affected applicant/employee to respond to the results of the Registry check.

D. If notification is received by the Superintendent or designee that that the applicant is listed as a perpetrator of abuse or neglect on the Registry, the Superintendent or designee shall provide the applicant with an opportunity to be heard regarding the results of the Registry check. If warranted by the results of the Registry check and any additional information provided by the applicant, the Superintendent or designee shall revoke the offer of employment and/or terminate the applicant's employment if he or she has already commenced working for the district.

III. Criminal Records Check Procedure

A. Each person hired by the district shall be required to submit to state and national criminal record checks within thirty (30) calendar days from the date of employment. Each person otherwise placed within a school under any public assistance employment program, employed by a provider of supplemental services pursuant to federal law or in a nonpaid, noncertified position completing preparation requirements for the issuance of an educator certificate, who performs a service involving direct student contact shall also be required to submit to state and national

criminal record checks within thirty (30) calendar days from the date such worker begins to perform such service. Record checks will be processed according to the following procedure:

1. No later than five (5) calendar days after the Superintendent or his/her designee has notified a job applicant of a decision to hire the applicant, or as soon thereafter as practicable, the Superintendent or his/her designee will provide the applicant with a packet containing all documents and materials necessary for the applicant to be fingerprinted by the Norwich Police Department. This packet shall also contain all documents and materials necessary for the police department to submit the completed fingerprints to the State Police Bureau of Identification for the processing of state and national criminal record checks. The Superintendent or his/her designee will also provide each applicant with the following notifications before the applicant obtains his/her fingerprints: (1) Agency Privacy Requirements for Noncriminal Justice Applicants; (2) Noncriminal Justice Applicant's Privacy Rights; (3) and the Federal Bureau of Investigation, United States Department of Justice Privacy Act Statement.

2. No later than ten (10) 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 by the Norwich Police Department. 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. The affected applicant/employee may notify the Superintendent or his/her designee in writing within five (5) calendar days that the affected/employee will challenge his/her criminal history record check. Upon written notification to the Superintendent or his/her designee of such a challenge, the affected applicant/employee shall have ten (10) calendar days to provide the Superintendent or his/her designee with necessary documentation regarding the affected applicant/employee's record challenge. The Superintendent or his/her designee may grant an extension to the preceding ten-day period during which the affected applicant/employee may provide such documentation for good cause shown.

5. Decisions regarding the effect of a conviction upon an applicant/employee, whether disclosed or undisclosed by the applicant/employee, will be made on a case-by-case basis. Notwithstanding the foregoing, the falsification or omission of any information on a job application or in a job interview, including but not limited to information concerning criminal convictions or pending criminal charges, shall be grounds for disqualification from consideration for employment or discharge from employment.

6. Notwithstanding anything in paragraph III.A.5 of this Policy, above, no decision to deny employment or withdraw an offer of employment on the basis of an applicant/employee's criminal history record shall be made without affording the applicant/employee the opportunities set forth in paragraph III.A.4 of this Policy, above.

B. **Criminal Records Check for Substitute Teachers:**

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

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

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

IV. Sex Offender Registry Checks

School district personnel shall cross-reference the Connecticut Department of Public Safety's sexual offender registry prior to hiring any new employee. Registration as a sexual offender constitutes grounds for denial of employment opportunities.

V. Credit Checks

The district may also ask a prospective employee for a credit report for employment for certain district positions, where the district's receipt of a credit report is substantially related to the employee's potential job. Substantially related is defined to mean "the information contained in the credit report is related to the position for which the employee or prospective employee who is the subject of the report is being evaluated." Prior to asking for a credit report, the district will determine whether the position falls within one of the categories as described in this paragraph. The position must: (1) be a managerial position which involves setting the direction or control of the district; (2) involve access to employees' personal or financial information; (3) involve a fiduciary responsibility to the district, including, but not limited to, the authority to issue payments, collect debts, transfer money or enter into contracts; (4) provide an expense account or district debit or credit card; or (5) involve access to the district's nonfinancial assets valued at two thousand five dollars or more.

When a credit report will be requested as part of the employment process, the district will provide written notification to prospective employee regarding the use of credit checks. That notification must be provided in a document separate from the employment application. The notification must state that the district may use the information in the consumer credit report to make decisions related to the individual's employment.

The district will obtain consent before performing the credit or other background checks. If the district intends to takes an action adverse to a potential employee based on the results of a credit report, the district must provide the prospective employee with a copy of the report on which the district relied in making the adverse decision, as well as a copy of "A Summary of Your Rights Under the Fair Credit Reporting Act," which should be provided by the company that provides the results of the credit check. The district will notify the prospective employee either orally, in writing or via electronic means that the adverse action was taken based on the information in the consumer report. That notice must include the name, address and phone number of the consumer reporting company that supplied the credit report; a statement that the company that supplied the report did not make the decision to take the unfavorable action and cannot provide specific reasons for the district's actions; and a notice of the person's right to dispute the accuracy or completeness of any information the consumer reporting company furnished, and to get an additional free report from the company if the person asks for it within sixty (60) calendar days.

VI. Notice of Conviction

If, at any time, the district receives notice of a conviction of a crime by (1) a person holding a certificate, authorization or permit issued by the State Board of Education, or (2) a person employed by a provider of supplemental services, the district shall send such notice to the State Board of Education.

VII. School Nurses

School nurses or nurse practitioners appointed by, or under contract with, the district shall also be required to submit to a criminal history records check in accordance with the procedures outlined above.

VIII. Personal Online Accounts

For purposes of these Administrative Regulations, "personal online account" means any online account that is used by an employee or applicant exclusively for personal purposes and unrelated to any business purpose of the district, including, but not limited to, electronic mail, social media and retail-based Internet web sites. "Personal online account" does not include any account created, maintained, used or accessed by an employee or applicant for a business purpose of the district.

A. During the course of an employment check, the district may not:

1. request or require that an applicant provide the district with a user name and password, password or any other authentication means for accessing a personal online account;

2. request or require that an applicant authenticate or access a personal online account in the presence of the district; or

3. require that an applicant invite a supervisor employed by the district or accept an invitation from a supervisor employed by the district to join a group affiliated with any personal online account of the applicant.

B. The district may request or require that an applicant provide the district with a user name and password, password or any other authentication means for accessing:

1. any account or service provided by district or by virtue of the applicant's employment relationship with the district or that the applicant uses for the district's business purposes, or

2. any electronic communications device supplied or paid for, in whole or in part, by the district.

C. In accordance with applicable law, the district maintains the right to require an applicant to allow the district to access his or her personal online account, without disclosing the user name and password, password or other authentication means for accessing such personal online account, for the purpose of:

1. conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an applicant's personal online account; or

2. conducting an investigation based on the receipt of specific information about an applicant's unauthorized transfer of the district's proprietary information, confidential information or financial data to or from a personal online account operated by an applicant or other source.

IX. Policy Inapplicable to Certain Individuals

This policy shall also not apply to:

A. A student employed by the district who attends a district school.

B. A person employed by the district as a teacher for a noncredit adult class or adult education activity, as defined in Conn. Gen. Stat. § 10-67, who is not required to hold a teaching certificate pursuant to Conn. Gen. Stat. § 10-145b for his or her position.

X. Falsification of Records.

Notwithstanding any other provisions of this policy, the falsification or omission of any information on a job application or in a job interview, including but not limited to information concerning abuse or neglect investigations or pending criminal applications, shall be grounds for disqualification from consideration for employment or discharge from employment.

Legal References: Conn. Gen. Stat. § 10-212

Conn. Gen. Stat. § 10-221d

Conn. Gen. Stat. § 10-222c

Conn. Gen. Stat. § 31-40x

Conn. Gen. Stat. § 31-51i

Conn. Gen. Stat. § 31-51tt

Public Act 18-51, "An Act Implementing the Recommendations of the Department of Education."

Elementary and Secondary Education Act, reauthorized as the Every Student Succeeds Act, Pub. L. 114-95, codified at 20 U.S.C.§ 1001 *et seq.*

Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.

ADOPTED: 12/20/94
REVISED: 6/19/07
REVISED: 6/13/17
REVISED: 5/8/18
REVISED: 12/11/18

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[1] 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.[2]

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.

If you need additional information or assistance, contact:

Connecticut Records:	**Out-of-State Records:**
Department of Emergency Services and Public Protection **State Police Bureau of Identification (SPBI)** **1111 Country Club Road** **Middletown, CT 06457** **860-685-8480**	**Agency of Record** **OR** **FBI CJIS Division-Summary Request** **1000 Custer Hollow Road** **Clarksburg, West Virginia 26306**

[1] Written notification includes electronic notification, but excludes oral notification.

[2] See 5 U.S.C. 552a(b); 28 U.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).

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[3] by Norwich Public Schools 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.[4]

- 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.[5]

- 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.)

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

Connecticut Records:	**Out-of-State Records:**
Department of Emergency Services and Public Protection	**Agency of Record**
State Police Bureau of Identification (SPBI)	**OR**
1111 Country Club Road	**FBI CJIS Division-Summary Request**
Middletown, CT 06457	**1000 Custer Hollow Road**
860-685-8480	**Clarksburg, West Virginia 26306**

[3] Written notification includes electronic notification, but excludes oral notification.
[4] See 28 CFR 50.12(b).
[5] See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 42 U.S.C. 14616, Article IV(c); 28 CFR 20.21(c), 20.33(d) and 906.2(d).

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).

Criminal History Record Information (CHRI)
Proper Access, Use and Dissemination Procedures

Purpose

The intent of the following policies is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention rules.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. The Norwich Public Schools may complement this policy with a local policy; however, the CJIS Security 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.

Scope

The scope of this policy applies to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location from the Norwich Public Schools. In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

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

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

Proper Access, Use, and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

Personnel Security Screening

Access to CJI and/or CHRI is restricted to authorized personnel. Authorized personnel is defined as an individual, or group of individuals, who have completed security awareness training and have been granted access to CJI data.

Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.

Physical Security

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.

Only authorized personnel will have access to physically secure non-public locations. The Norwich Public Schools will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting 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.

Media Protection

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

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

Media Transport

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Media Sanitization and Disposal

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

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

1) shredding using Norwich Public Schools issued shredders.

2) placed in locked shredding bins for Norwich Public Schools to come on-site and shred, witnessed by Norwich Public Schools personnel throughout the entire process.

3) incineration using Norwich Public Schools incinerators or witnessed by Norwich Public Schools personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

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

1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

2) **Degaussing -** a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

3) **Destruction –** a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from Norwich Public Schools's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

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

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

Remote Access

The Norwich Public Schools shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

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

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

Personally Owned Information Systems

A personally owned information system 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 any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

Reporting Information Security Events

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

Policy Violation/Misuse Notification

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

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