

## **BACKGROUND INVESTIGATION AND CRIMINAL HISTORY RECORDS CHECK- INTERNAL CONTROLS AND PROCEDURES**

- A. Purpose.** This procedural document outlines the responsibilities and protocols required relative to receipt, access, retention and destruction of criminal history record information obtained through the criminal history records check required under RSA 189:13-A and Board policy GBCD.
- B. Definitions.** Except as noted relative to New Hampshire law or Board policy, the definitions are based on those provided in the Criminal Justice Information Services Security Policy, of the Federal Bureau of Investigation, Criminal Justice Information Services Division (the "CJIS Security Policy").
1. Criminal Justice Information ("CJI") – refers to all of the data provided through the Federal Bureau of Investigation's ("FBI") criminal justice information system ("CJIS") including, but not limited to biometric, identity history, biographic, property, and case/incident history data.
  2. Criminal History Records Information ("CHRI") – is a subset of CJI, including: information, notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges. For purposes of this document GBCD-RG, CHRI will also include all of the information received through the New Hampshire State Police pursuant to RSA 189:13-a regarding the criminal history of a "covered person" GBCD whether or not such information is received by or through the CJIS.

Due to its sensitive nature, and pursuant to regulations of the FBI, additional controls beyond those stated in RSA 189:13-a are required for the access, use and dissemination of CHRI.

3. "Authorized Person" & "Authorized Personnel" - an individual ("Authorized Person"), or group of individuals ("Authorized Personnel"), who have been appropriately vetted through a national fingerprint- based record check and have been granted access to CHRI data. However, pursuant to RSA 189:13-a, only the Superintendent or her/his "Designee" as defined under Board policy GBCD qualify as "Authorized Personnel". See Section D, below for requirements for training of Authorized Personnel.
4. 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.
5. Physical Media - includes printed documents and imagery.

**C. Designated Points of Contact.**

Each Authorized Person may serve as a point of contact ("POC") for communications with the FBI, or with the New Hampshire State Police, Justice Information Bureau, as the state CJIS agency ("CSA"), regarding such matters as (i) CHRI audits, (ii) changes to Authorized Personnel within the District, (iii) CHRI training, or (iv) CHRI security as required under state or federal law.

In the event the District has only one Authorized Person, the Superintendent shall also designate a person other than the Authorized Person to serve as an "Alternate POC". Such Alternate POC will not have access to CHRI (i.e., the Alternate POC is not an "Authorized Person"), but may engage in communications as described in this paragraph, especially in the absence of an Authorized Person. (Hereafter, the/a "POC" will mean and include any Authorized Personnel as well as the Alternate POC.) In addition to communications with the CSA and FBI as described above, the POC will support policy compliance, including such matters as:

1. Using the New Hampshire State Police Criminal Records Portal (the "NH Criminal Records Portal"), documentation of approved hardware, software, and firmware;
2. Using the NH Criminal Records Portal, communications regarding how the District's devices/network are connected to the Criminal Records Portal; and
3. Implementation and compliance with security procedures.

**D. Training of Authorized Personnel.**

The District will ensure that each Authorized Person will complete the training relative to the reading and interpretation of criminal records as required under RSA 189:13-a. Additionally, the District will ensure all persons authorized to have CHRI access will complete Security Awareness Training via CJIS Online immediately upon hire or appointment to access CHRI.

The District will ensure all Authorized Personnel complete recertification of Security Awareness Training every twelve (12) months.

The Alternate POC will keep on file the Security Awareness Training certificate on all authorized personnel.

**E. Termination or other Changes to Authorized Personnel.**

Upon an Authorized Person's separation/termination from employment with the District, a POC shall, as soon as practicable, terminate the separated employee's access to systems or physical areas that would allow access to CHRI. In the event that there are any other additions or reductions to district employees assigned or to be assigned as Authorized Personnel, the POC will notify the CSA of the personnel changes within seven business days.

Each POC will keep an updated list of the Authorized Personnel and POC that will be available to the CSA or FBI.

**F. Access to, and Security, Storage, Retention and Destruction of CHRI.**

1. Access to and Storage of CHRI. Authorized Personnel as defined in section B.3, above, are the only persons allowed to access, view, possess, or otherwise handle CHRI whether in physical or electronic media. Any other dissemination of CHRI in any format or medium is strictly forbidden.

The Superintendent shall designate an area, a room, or a storage container as a controlled area for the purpose of day-to-day access to or storage of CHRI on physical media. CHRI on physical media will be stored at all times in a locked drawer/container at the Central Office that is only accessible to the Authorized Personnel. CHRI in physical media shall not be removed from the designated area except for destruction as provided below.

Any room, area or storage container in which CHRI is contained on physical media shall be locked whenever unattended by Authorized Personnel.

Documents or other physical media containing CHRI, and any devices through which CHRI on electronic media may be viewed, will be positioned at all times in such a way as to prevent persons who are not Authorized Personnel from accessing or viewing CHRI.

In no event shall any physical media containing CHRI be copied or transferred to any electronic media. Similarly, CHRI received and/or accessed through the New Hampshire State Police Criminal Records Portal (the "Criminal Records Portal"), shall not be transferred to physical media (e.g., printed), and shall not be saved or transferred onto any other electronic media or device.

Additionally, if CHRI is received or accessed through the Criminal Records Portal, the District will at all times use electronic media and network infrastructure security methods consistent with the CJIS Security Policy and/or as otherwise required by the CSA or FBI.

The District shall take steps necessary to prevent and protect the District from physical, logical, and electronic breaches consistent with the District's Data Governance and Security Plan and Board policy EHAB.

In no event shall a "personal device" or "personally owned information system" be used to access, view, process, store or transmit CHRI. For the purposes of this policy, "personal device" or "personally owned information system" shall include any portable technology, including, but not limited to, mobile wireless devices (e.g., Blackberries, cellphones, smart phones, tablets, etc.), personal laptops, personal desktop computers, or portable storage device (e.g., flash drive, SD card, DVD, CD, air card, etc.).

2. CHRI Exempt from Public Disclosure. CHRI is exempt from disclosure to the public under RSA 91-A:5, IV. See also, Section 4.2.1 of the CJIS Security Policy, stating that CHRI obtained from the Interstate Information Index is only accessible for an authorized purpose; and FOIA(b)(7)(c), stating that matters which are an unwarranted invasion of personal privacy are exempt from disclosure.

3. Destruction of CHRI. The District will properly sanitize or destroy physical media or electronic media with CHRI within 60 days of receipt by the District. All CHRI will be destroyed as set out below.
  - a. Physical media with CHRI shall be destroyed by one of the following:
    - i. shredding by Authorized Personnel using District-issued cross-cut shredders;
    - ii. placed in locked shredding bins for a private contractor approved by the Superintendent to come on-site and shred, witnessed by District personnel throughout the entire process; or
    - iii. incineration using District incinerators or, if conducted by non-Authorized Personnel offsite, witnessed by the Superintendent or Superintendent's designee.
  - b. CHRI on electronic media shall be removed or destroyed by one of the below methods, and computers and other digital or electronic devices or systems that have been used to process, store, or transmit sensitive information shall not be released from the District's direct control until all CHRI has been destroyed using one of the prescribed methods:
    - i. Overwriting (at least three times);
    - ii. Degaussing (magnetic or electric removal of magnetic data); or
    - iii. Physical destruction (i.e., dismantling by methods of crushing, disassembling, etc., ensuring that the platter or other storage device has been physically destroyed so that no data can be extracted).

**G. Reporting Information Security Events.**

The District will report information security events/cybersecurity incidents involving CHRI consistent with Board policy EHAB. Additionally, the District shall promptly report incident information to appropriate authorities, including the New Hampshire State Police CSA Information Security Officer (ISO).

**H. Violations - Misuse of CHRI.**

In the event of misuse of CHRI, or violations of any provision of (a) these Internal Controls and Procedures, or (b) the CJIS Security Policy, the District will subject the employee to disciplinary action per Board policy and procedures, up to and including the termination of their employment, and the employee may face criminal prosecution.