LEBANON SCHOOL DISTRICT

POLICY: 800.1
SECTION: OPERATIONS
TITLE: CONFIDENTIALITY AND SECURITY OF FBI CRIMINAL HISTORY RECORD INFORMATION
ADOPTED: September 17, 2018
LAST REVISED: April 20, 2020

800.1. CONFIDENTIALITY AND SECURITY OF FBI CRIMINAL HISTORY RECORD INFORMATION

Purpose

As a supplement to the General Background Checks and Related Requirements set forth and required in Policy Section 300[1] and Policy 916, the intent of this document is to set forth procedures to be followed by the District to help ensure protection of Criminal History Record Information provided through systems administered by the FBI (referred to herein as "**CHRI**"). The procedures were developed based on the FBI Criminal Justice Information Services Security Policy.

Scope

The procedures apply to any electronic or physical media containing CHRI while being stored, accessed, or physically moved or destroyed by the District or a District employee or agent. In addition to the procedures set forth below, Title 28, Part 20, Code of Federal Regulations provides regulatory guidance. The District may, but is not required to apply similar procedures to Criminal History Record Information obtained from the Pennsylvania State Police.

Confidentiality of CHRI

CHRI is considered confidential information and shall be treated as such by the District and all District employees and agents. As a result of confidentiality, CHRI shall be made available only to authorized personnel and used only for lawful purposes related to background checks.

[1] 24 P.S. 111; 23 Pa.C.S.A. 6301 et. seq.; 22 Pa. Code. 8.1 et. seq.

Proper Access, Use, and Dissemination of CHRI

The District will not disseminate CHRI to any other entity or to an individual other than authorized personnel. For employees or agents of independent contractors for whom CHRI is required as a condition of providing services to the District, the District will review the CHRI and transmit an acceptability or unacceptability determination to the independent contractor. If the independent contractor wishes to obtain a copy of the CHRI, the independent contractor should require its employee or agent to provide the unofficial copy of the CHRI to the independent contractor.

Personnel Security Limitations

Access to CHRI obtained or stored by the District is restricted to specifically authorized personnel determined based on job function and need to know in order to fulfill lawful purposes related to background checks. Legal counsel to the District shall be considered authorized personnel. The District will maintain a list either by position or name of authorized personnel other than legal counsel.

Security Awareness Training

Basic security awareness training shall be required within six (6) months of initial employment, and every two (2) years thereafter, for all authorized personnel. The District shall maintain a record of training by each authorized person. Training may consist of review of a video or PowerPoint accessible on the internet website of the Pennsylvania State Police.

Physical Security

CHRI will be stored or accessed only in a physically secure location. A physically secure location is an area within a facility with both physical and personnel security controls sufficient to protect CHRI and associated information storage and systems. Only authorized personnel will have access to the physically secure location. Authorized personnel will take reasonable steps to prevent and protect against physical or electronic breaches.

Media Protection

The District will establish controls to protect electronic and physical media containing CHRI while stored or actively being accessed. "**Electronic media**" incudes 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 drive, external hard drive, or digital memory card. "**Physical media**" includes printed documents and imagery that contain CHRI. The District will securely maintain electronic and physical

media within the physically secure location and restrict access to authorized personnel.

Media Transport

Controls shall be in place to protect electronic and physical media containing CHRI while in transport to prevent inadvertent or inappropriate disclosure.

Media Sanitization and Disposal

When no longer usable or subject to a retention requirement, electronic and physical media will be properly disposed of in accordance with the following measures.

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

1. **Shredding** – shredding by authorized personnel.

2. **Shredding** – placing in locked shredding bins for a private contractor to come on-site and shred, witnessed by authorized personnel.

Electronic media shall be disposed of by one of the following methods:

1. **Overwriting (at least 3 times)** – an effective method of clearing data from magnetic media. 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.

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

Account Management

The District shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The District shall validate information system accounts at least annually and shall document the validation process. All accounts shall be reviewed at least annually by a designated person to ensure access and account privileges

commensurate with job functions, need-to-know, and employment status on systems that contain CHRI.

Remote Access

The District prohibits remote access to CHRI by means of personally owned computers or other information systems. However, this shall not be interpreted to prohibit forwarding CHRI electronically or otherwise to legal counsel.

Personally Owned Information Systems

The District prohibits use of a personally owned information system to access, process, store, or transmit CHRI.

Reporting Information Security Breach

The District shall promptly report information concerning a CHRI security breach to appropriate Pennsylvania state authorities. All employees shall promptly report to the District Superintendent or designee any security breach.

Policy Violation/Misuse Notification

Violation of these procedures may result in disciplinary action applicable to an employee or visitor, including but not limited to loss of access privileges, civil and criminal prosecution, or termination of employment, or other appropriate action.

This policy/document will be signed by all employees who are authorized personnel.

BY MY SIGNATURE BELOW, I acknowledge receipt and review of this document.

Date: _____ _____

Employee Signature

_____

Employee Printed Name

_____

Employee Title