Urban Pathways K-5 College Charter School

Board of Trustees Policy

CRIMINAL HISTORY RECORD INFORMATION (CHRI) POLICY

Purpose

The Urban Pathways K-5 College Charter School ("Charter School") Board of Trustees' ("Board") intent of this policy is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until the information is purged or destroyed in accordance with applicable record retention rules.

Scope

This policy applies to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location within the Charter School. 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 refers 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 (or entity) 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.

The Charter School will maintain a list of authorized users.

Security Awareness Training

Basic security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel with access to said confidential information.

Physical Security

All CJI and CHRI information shall be securely stored. The Charter School will maintain a current list of authorized personnel. Authorized personnel will take necessary steps to prevent and protect the Charter School 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 Charter School shall securely store electronic and physical media within physically secure locations. The Charter School restricts 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. When no longer usable, information and related processing items shall be properly disposed of to ensure confidentiality.

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 Charter School shall protect and control electronic and physical media during transport outside 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 the Charter School.

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

1) shredding using Charter School issued shredders. Shredding must be completed by authorized personnel.

2) placed in locked shredding bins for a private contractor to come on-site and shred, witnessed by authorized personnel during the entire process.

Electronic media (hard-drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the Charter School's 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 degaussers. 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 the Charter School's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

The Charter School shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The Charter School shall validate information systems 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), which is the CEO or designee to ensure that access and account privileges are 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 Charter School 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 the Charter School's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The Charter School 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.

Reporting Information Security Events

The Charter School 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.

Operational Records Division
Bureau of Records and Identification
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110
(717) 783-5599

Formal event reporting and escalation procedures shall be in place. Wherever feasible, the Charter School 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 Charter School assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact, which is the CEO or designee.

Policy Violation/Misuse Notification

Violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any person can result in significant 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.

Criminal History Record Information (CHRI) Proper Access, Use and Dissemination Policy & Procedure List

Upon adoption of this Policy, the Charter School will maintain a list of signatures of all authorized persons, including, but not limited to, such authorized persons who are employees, staff and contracted persons, for their signatures showing their certification that they were given a copy of the instant policy, along with the opportunity to discuss and ask questions on the above topics.

Any complaints with regard to a Board policy or any aspect of the Charter School's curriculum shall be brought in accordance with the Charter School's Complaint Policy.

TO THE EXTENT THAT ANYTHING IN THIS POLICY COULD BE CONSTRUED TO CONFLICT WITH THE CHARTER SCHOOL'S CHARTER OR APPLICABLE STATE AND/OR FEDERAL LAWS, THE APPLICABLE STATE AND/OR FEDERAL LAWS AND/OR CHARTER CONTROL.

BY MY SIGNATURE BELOW, I CERTIFY THAT I HAVE BEEN GIVEN A COPY OF THE CRIMINAL HISTORY RECORD INFORMATION (CHRI) POLICY AND HAVE BEEN GIVEN THE OPPORTUNITY TO DISCUSS AND ASK QUESTIONS ON THE ABOVE TOPICS.

Employee Printed Name: _____

Employee Signature: _____

Employee Title: _____

Date: _____