Criminal History Record Information

PURPOSE

The District may use Criminal History Record Information (CHRI) obtained from the Kentucky State Police (KSP) to check qualification for employment or service as provided in KRS 160.380 and related policies and for authorizing personnel who will make fitness determinations. CHRI may not be used for any other purpose.

AUTHORITY

The District has the authorization to submit fingerprints to KSP for a fee-based state and federal background check pursuant to KRS 160.380.

NONCRIMINAL JUSTICE AGENCY CONTACT (NAC) & LOCAL AGENCY SECURITY OFFICER (LASO)

The Superintendent will designate employee(s) to serve as the NAC and LASO points of contact with KSP through which communication regarding audits, District personnel changes, training, and security are conducted. The NAC and LASO will receive and disseminate communication from KSP to all authorized District personnel. Additionally, the LASO shall where applicable:

1. Identify who is using the Criminal Justice Information Services (CJIS) Systems Agency (CSA) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated.
4. Ensure approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA Information Security Officer is promptly informed of security incidents.

AUTHORIZED PERSONNEL

Authorized personnel will be given access to view and handle CHRI after completing the required Security Awareness Training and any additional training required by KSP. Only authorized personnel may access, discuss, use, possess, disseminate, or destroy CHRI.

The District will keep an updated list of authorized personnel that will be available to the KSP Auditor during the audit process.

TRAINING OF AUTHORIZED PERSONNEL

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 NAC will keep on file the Security Awareness Training certificate on all authorized personnel.

The District will ensure authorized users complete recertification of Security Awareness Training every twelve (12) months.

Authorized personnel will review the KSP website Noncriminal Justice Agency (NCJA) section for policies, procedures, and forms necessary for CHRI handling and fitness determination.

Criminal History Record Information

FINGERPRINT CARD PROCESSING

The District requires that all covered persons for whom fingerprint check is required must provide a valid, unexpired form of government-issued photo identification prior to fingerprinting to verify their identity.

A copy of the FBI Privacy Rights Notification will be provided to the covered persons prior to fingerprinting. Covered persons will also be advised of the process regarding a challenge of the criminal history record.

Covered persons that have disclosed a conviction must still be fingerprinted. Proper reason for fingerprinting must be documented in the "Reason for Fingerprinting" box.

Proper chain of custody procedures protecting the integrity of the covered person's fingerprints prior to submission will include maintaining fingerprints in a secure environment, in a sealed envelope.

COMMUNICATION

Authorized personnel may discuss the CHRI results with covered persons in a secure, private area. Extreme care will be taken to prevent overhearing, eavesdropping, or interception of communication.

The District will not allow a covered person to have a copy of their record or take a picture of it with an electronic device.

The District will provide the covered person with required forms and options to obtain their record if a record is to be challenged.

PHYSICAL SECURITY

The District will ensure that information system hardware, software, and media are physically protected through access control measures by ensuring the perimeter of a physically secured location shall be prominently posted and separated from non-secure locations by physical controls. The District will control all access points (except for those areas within the facility officially designated as publicly accessible) and will verify individual access authorizations before granting access. The District will control physical access to information system distribution and transmission lines within the physically secure location. The District will control physical access to information system devices that display Criminal Justice Information (CJI) and will position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI. The District will monitor physical access to the information system to detect and respond to physical security incidents. The District will control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible) and will escort visitors in a secured location.

Criminal History Record Information

STORAGE AND RETENTION OF CHRI

The fingerprint results from KSP should only be handled by authorized personnel.

During the fitness determination:

- CHRI will be stored in a locked drawer/container at the Central Office and only accessible to authorized personnel.
- CHRI will be stored in a separate file that cannot be released for any public records request and will not be archived in a publicly accessible location.
- CHRI results will be stored electronically the agency using proper security and encryption methods.
- If stored electronically, the District will ensure compliance of CJIS Security Policy for the Network Infrastructure to include the following:
    1. Network Configuration
    2. Personally Owned Information Systems
    3. Publicly Accessible Computers
    4. System Use Notification
    5. Identification/User ID
    6. Authentication
    7. Session Lock
    8. Event Logging
    9. Advance Authentication
    10. Encryption
    11. Dial-up Access
    12. Mobile Devices
    13. Personal Firewalls
    14. Bluetooth Access
    15. Wireless (802.11x) Access
    16. Boundary Protection
    17. Intrusion Detection Tools and Techniques
    18. Malicious Code Protection
    19. Spam and Spyware Protection
    20. Security Alerts and Advisories
    21. Patch Management
    22. Voice over Internet Protocol (VoIP)
    23. Partitioning and Virtualization
    24. Cloud Computing
- Per KRS 61.878, CHRI is not subject to disclosure under the Kentucky Open Records Act and will not be archived in a publicly accessible location.

Criminal History Record Information

MEDIA TRANSPORT

The District will protect and control digital and physical media during transport outside of controlled areas and will restrict the activities associated with transport of such media to authorized personnel.

DISPOSAL OF MEDIA CHRI

The District will properly sanitize or destroy physical or electronic CHRI per the Kentucky Department of Libraries and Archives (KDLA) Public School District Records Retention Schedule. If a third party performs the destruction, an authorized person shall accompany the CHRI through the destruction process. For electronic media, the District shall overwrite three (3) times or degauss digital media prior to disposal or release, inoperable digital media shall be destroyed; cut up, shredded, etc. The District shall ensure the sanitation or destruction is witnessed or carried out by authorized personnel.

MISUSE OF CHRI

In the event of deliberate or unintentional misuse of CHRI, the District will subject the employee to disciplinary action per Board policy and procedures, up to and including termination, or request for criminal investigation/charges.

Review/Revised:6/19/2023