The Leadership School
STUDENT LEADERSHIP AT THE CENTER OF LEARNING

Policy for Access and Use of Fingerprint-Based Criminal History Record Information (CHRI)

Use:

In accordance with the National Child Protection Act of 1993, as amended and R.S.Mo 168.133, **The Leadership School** will ensure that a state and national fingerprint-based criminal background check is conducted on any person authorized to have contact with pupils and prior to the individual having contact with any pupil. Such persons include, but are not limited to, LEA employees (administrators, teachers, assistants, paraprofessionals, office staff), contractors, and volunteers for the purpose of employment and/or access to children.

Definitions:

Criminal History Record Information (CHRI) - An individual's criminal history obtained through the systems of the Missouri State Highway Patrol (MSHP) and/or the Federal Bureau of Investigation (FBI) via submission of the individual's fingerprints. CHRI includes information on the individual's demographics, arrest(s), prosecution(s), disposition(s), and detention(s) pertaining to reportable criminal charges.

Security violation - The act of violating, knowingly or not, a security policy regarding CHRI. Security violations include, but are not limited to: CHRI systems/data misuse; virus/malware/ransomware attacks; network intrusion; data loss/data breach; unauthorized access to CHRI systems; denial of service; unauthorized changes; and theft/loss of devices containing CHRI.

Local Agency Security Officer (LASO) - The security point of contact between the user agency and the MSHP. The LASO is appointed by the Agency Head.

Authorized Personnel - Personnel determined by the Agency Head or designee to require access to or otherwise view CHRI in official capacity with the agency.

Secured environment - A secure storage area for hard copy and/or electronic media CHRI. A secured environment includes, but is not limited to, a locking drawer or filing cabinet; locking vault; or lockbox.

Electronic format - Text-based or image-based content in a form that is produced on, published by, and readable on Personal Computers (PCs) or other digital devices. Electronic formats include, but are not limited to, portable document format (PDF); Microsoft Word; Text (TXT); Joint Photographic Experts Group (JPEG); and Portable Network Graphics (PNG) file formats.

Electronic media - Media that use electronics or electromechanical means for a user to access electronic format content. Electronic media includes, but is not limited to, computer Hard Disk Drives (HDDs); computer Solid State Drives (SSDs); portable flash sticks/drives; compact discs (CDs); and digital versatile discs (DVDs).

Optical media disc - Electronic media that stores electronic format content on an optical disc and includes CDs and DVDs.

Degauss - The destruction of data stored on certain electronic media such as HDDs, SSDs, and portable flash sticks/drives.

Applicant Privacy Rights

Prior to fingerprints being captured, the employee or volunteer must be provided a copy of the "Noncriminal Justice Applicant's Privacy Rights" and the FBI's "Privacy Act Statement." When registering for fingerprinting through the MACHS portal, this information is provided and acknowledged during the registration process. If not registering through the Patrol's MACHS portal, the agency will provide a hard copy to the applicant.

Waiver Agreement and Statement - For VECHS Participation Agencies - the VECHS Waiver must be completed, signed and dated and retained at the agency.

Security Violations

The Leadership School will ensure the CHRI received is protected from receipt until destruction and will establish appropriate technical and physical precautions to secure the CHRI.

If a security violation occurs with CHRI, whether malicious in intent or not, the violation will be reported to **The Leadership School**'s LASO. The LASO will complete a MSHP SHP-71 Security Incident Report form and forward the completed form to the MSHP Criminal Justice Information Services (CJIS) Security Unit.

The Leadership School designates the following individual to act as the LASO:

Dr. Kimberly Townsend,
Executive Director
1785 Pennsylvania Ave St. Louis, MO 63133
314-492-2301/ 314-
ktownsend@tlsstl.org

Security Awareness Training

To comply with Appendix J of the FBI CJIS Security Policy, basic security awareness training is required prior to initial assignment or access to Criminal Justice

Information (CJI), and annually thereafter. **The Leadership School** completes security awareness training via **CJIS Online** and proof of completed and current security awareness training will be retained indefinitely for all personnel with access to CHRI.

Access, Use, and Retention of CHRI

Only authorized personnel of **The Leadership School** may access, view, or otherwise use CHRI and shall not share or disclose CHRI to unauthorized personnel. If CHRI is printed in a hard copy format, authorized personnel will ensure the information is stored in a secured environment and is not accessible by unauthorized personnel. The security combination and/or keys to the locks shall only be accessible by authorized personnel. If CHRI is stored in an electronic format, the electronic media will be treated the same as hard copy CHRI and will be stored in a secure environment that is not accessible by unauthorized personnel. If the electronic media cannot be stored in a secure environment, such as being stored on a PC's local HDD or SSD, the electronic CHRI must be password-protected or otherwise encrypted.

Destruction of CHRI

When hard copy CHRI or electronic CHRI stored on optical media discs is no longer required, it must be destroyed in one of the following manners:

- In-House Cross Shredder
- Incineration
- Contracted Document Destruction Company

If a contracted document destruction company is used, authorized personnel must accompany the CHRI to destruction.

When electronic copy CHRI stored on HDDs, SSDs, or flash sticks is no longer required, the electronic media must be degaussed a minimum of three times.

Dissemination

The Leadership School will not dissemination CHRI; or

The Leadership School will disseminate to the applicant of record for personal review or challenge purposes only. The request must be in writing and the applicant must appear in person, with identification, and sign a secondary dissemination log.

Authorized personnel will document when CHRI is disseminated to the subject of the record on a secondary dissemination log. In addition, authorized personnel will ensure CHRI is not disseminated to unauthorized personnel. Secondary dissemination logs will include, at a minimum: the date of secondary dissemination,

the name of the subject of the record, the name of the person or agency requesting the record, a description of the shared record, the purpose of the request, how the dissemination occurred, and the name of the disseminator. The secondary dissemination log will be retained for at least 3 years or until a compliance audit can be conducted by the MSHP.

MACHS Portal Access

The Leadership School will ensure all MACHS portal access is current. Any user that no longer needs access will be removed immediately by the Agency LASO or the MACHS Administrator.

The Leadership School LASO will contact the Missouri State Highway Patrol, CJIS Division, Trainer/auditor for assistance with Administrator rights to the MACHS portal.

Rap Back Participation

The Leadership School will ensure that Rap Back subscriptions are kept up-to-date and removed when the applicant is no longer working or volunteering for the agency. Rap Back subscriptions and validations will be conducted by the MACHS administrator of the agency.