New Policy #45-A: Background Checks & Fingerprinting Policy

1. Any employee, member of the Board shall complete a criminal background check and a check of the family care safety registry.

2. Any volunteer or individual otherwise authorized to have contact with students (and prior to any individual having contact with students) shall complete a criminal background check (if student contact is unsupervised by a School employee) and a check of the family care safety registry (if student contact is supervised by a School employee).

3. In order to facilitate the criminal background check and check of the family care safety registry, any employee, member of the Board, volunteer, or individual otherwise authorized to have contact with students (and prior to any individual having contact with students) shall complete a state and national fingerprint based criminal background check.

4. 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.

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

6. If a security violation occurs with information provided by the fingerprint background check, whether malicious in intent or not, the violation will be reported to the School's Local Agency Security Officer (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.

7. The School designates the following individual to act as the LASO: Mr. Ryan Brennan, Chief Operating Officer.

8. To comply with Appendix J of the FBI CJIS Security Policy, basic security awareness training is required for all personnel who have access to Criminal Justice Information (CJI) within six months of initial assignment, and biennially thereafter. The School completes security awareness training via [hard copy, CJIS Online, etc.] and proof of completed and current security awareness training will be retained indefinitely for all personnel with access to information provided from the fingerprint background checks.

9. Only authorized personnel of the School may access, view, or otherwise use information provided from the fingerprint background check and check of the

family care safety registry and shall not share such information from any individual not authorized to access, view, or otherwise use the information. If such information is printed on 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 such information is stored in an electronic format, the electronic media will be treated the same as hard copy information 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 information must be password-protected or otherwise encrypted.

10. When hard copy information or information stored on optical media discs is no longer required, it must be destroyed in one of the following manners:
    a. In-House Cross Shredder
    b. Incineration
    c. Contracted Document Destruction Company. If a contracted document destruction company is used, authorized personnel must accompany the CHRI to destruction.

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

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

13. The 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.

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

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