Personnel

Security Check/Fingerprinting

To create a safe and orderly environment for students, all offers of employment will be conditional upon the successful outcome of a criminal record check. In addition, any person applying for employment with The Academy shall submit to a record check of the Department of Children and Families (DCF) Child Abuse and Neglect Registry before the person may be hired.

Applicants, as required, shall make disclosures containing (1) current and past employers' contact information; (2) authorization allowing contact with such employers; and (3) statements about any past misconduct, discipline, or licensure penalties as a result of sexual misconduct or abuse allegations.

The Academy, before hiring such applicants, will ensure that they complete the above-stated three requirements and review the applicants' employment history after making a documented, good-faith effort to contact previous employers for information.

All Academy employees shall submit to state and national criminal checks within 30 days after they are hired. District students employed by the school system are exempted from this requirement.

Student teachers placed in District schools as part of completing preparation requirements for issuing an educator certificate shall also be required to undergo the same criminal background checks and DCF child abuse and neglect registry check already required for school employees.

Criminal Justice Information (CJI) is to be maintained in accordance with the administrative regulation pertaining to the use and disclosure of criminal justice information.

Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)
This policy applies to any electronic or physical media containing FBI CJI while stored, accessed, or physically moved from a secure location at The Academy. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

CJI refers to all 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 policy, is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use, and dissemination of CHRI.

Proper Access, Use, and Dissemination of CHRI
Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing CHRI's access, use, and dissemination 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 is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) if 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 appropriately vetted through a national fingerprint-based record check and granted access to CJI data. Agencies

(including school districts located within states with legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to CHRI for the purposes of licensing or employment) shall submit a fingerprint-based record check within 30 days of employment or assignment on all personnel who have direct access to CJI, those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI, and any persons with access to secure locations or controlled areas containing CJI.

Security Awareness Training
Basic security awareness training is required within six months of initial assignment and biennially thereafter for all personnel with access to CJI.

Physical Security
A "physically secure location" is a facility or an area, room, or group of rooms within a facility with sufficient physical and personnel security controls to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

Only authorized personnel shall access physically secure non-public locations. The Academy will maintain a current list of authorized personnel. Authorization is required before any access to The Academy's secure areas or physical access points is granted. The Academy will implement access controls and monitor physically secure areas to protect all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect The Academy 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 cards. "Physical media" includes printed documents and imagery that contain CJI.

The Academy shall securely store electronic and physical media within physically secure locations or controlled areas. The Academy 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.

Media Transport
Controls shall 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 Academy shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with the transport of such media to authorized personnel.

Media Sanitization and Disposal
When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, 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 Academy.

Account Management
The Academy shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The Academy shall validate information system 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) or his/her 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.

Personally Owned Information Systems

A personally owned information system is not authorized to access, process, store, or transmit CJI unless The Academy has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes any portable technology like a camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards, and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops, any personal desktop computer, or other digital devices.

Reporting Information Security Events

The Academy shall promptly report incident information to appropriate authorities, including the state CSA or SIB's Information Security Officer (ISO). Information security events and weaknesses associated with information systems shall be communicated to allow for timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, The Academy shall employ automated mechanisms to assist in reporting security incidents. All employees shall be made aware of the procedures for reporting the different types of events and weaknesses that might impact the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Policy Violation/Misuse Notification

Violation of any of the requirements contained in this CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and/or termination.

Violating 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 result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181 and June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67)
29-17a Criminal history checks. Procedure. Fees.
PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records
Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.
CJIS Security Policy
Title 28 C.F.R. Part 20

Policy Adopted: February 23, 2010
Policy Updated: November 18, 2014
Policy Updated: October 17, 2023

The Woodstock Academy
Woodstock, Connecticut