Personnel

Use and Disclosure of Criminal Justice Information

Each applicant for a position with the District shall be required to submit to state and national criminal record checks in accordance with the District's Employment Checks Policy and applicable law. In addition, certain volunteers may also be required to submit to state and national criminal record checks in accordance with the District's Volunteers Policy. All results and accompanying information shall be considered "Criminal Justice Information" or "CJI" (each as more fully defined herein) and shall be maintained, used and disclosed in accordance with these regulations.

A. Definition and Scope

For purposes of these regulations:

"*Criminal Justice Information*" or "CJI" means the results of any state or federal criminal records check of an employee, contractor or volunteer, any applicant or prospective employee, contractor or volunteer, and all copies thereof.

"*Criminal Justice Information Officer* or "*CJI Officer*" means the individual appointed by the Superintendent to be responsible for the use, disclosure and safeguarding of CJI in the District, and to serve as the District's primary point of contact for matters relating to CJI and these regulations.

"*Permitted Individual*" means an individual designated by the Superintendent, or his or her designee, who may access CJI. Permitted Individuals may include, but shall not be limited to, District human resources personnel, certain administrators and certain administrative staff.

These regulations apply to all CJI in the possession or control of the District, in any form or format, including but not limited to CJI incorporated or contained in correspondence, documentation or reports of the District.

B. Responsibility

The Director of Human Resources shall serve as the District's CJI Officer unless the Superintendent appoints a different individual as the CJI officer.

C. Requesting Criminal Justice Information

The District shall request CJI from an employee, contractor, applicant or volunteer or potential employee, contractor or volunteer only as permitted or required by law or District policy.

D. Use of Criminal Justice Information

1) The Superintendent, or his/her designee, shall designate those individuals who shall be considered Permitted Individuals for purposes of these regulations. No other District employee or staff person may access or use CJI for any reason without obtaining prior written approval from the CJI Officer or his/her designee. A Permitted Individual shall use CJI only as permitted or required by District policy or law.

2) The District shall ensure that each Permitted Individual satisfies the applicable legal screening requirements prior to granting the Permitted Individual access to CJI, including:

- If the Permitted Individual is a resident of Connecticut, the District shall screen the Permitted Individual through a Connecticut and national fingerprint-based record check within 30 days of designation as a Permitted Individual; or

- If the Permitted Individual is not a resident of Connecticut, the District shall conduct state and national fingerprint-based record checks and follow FBI guidance regarding additional screening requirements.

The CJI Officer may consult with the Connecticut Department of Emergency Services and Public Protection on execution of the screening requirements.

3) The District may immediately terminate a Permitted Individual's access to CJI, with or without cause at the discretion of the Superintendent, CJI Officer, or their designees, and the District shall immediately terminate a Permitted Individual's access to CJI upon termination of the Permitted Individual's employment or contract with the District. The District shall reconsider a Permitted Individual's continued access to CJI upon any reassignment or modification to professional responsibilities.

E. Maintenance and Safeguarding

1) CJI shall be maintained in only the physically-secure locations, files and information systems designated by the District (the "Controlled Areas"). The Controlled Areas shall be limited to only Permitted Individuals or other authorized personnel and locked when unattended.

2) The District shall restrict access to CJI to only Permitted Individuals. In the event the District determines that it is unable to reasonably restrict access in accordance with this Section, all CJI shall be maintained in encrypted format, in a manner consistent with then-current legal requirements and industry standards.

3) No District employee may remove CJI from a Controlled Area without prior written approval of the CJI Officer. In the event the transport of CJI out of a Controlled Area is necessary for a legitimate function or activity, the CJI Officer shall develop a protocol to ensure the protection the CJI while in transport and while outside of the Controlled Area.

4) The District shall implement the following safeguards for CJI maintained in paper format: (i) maintain paper records in a physically secure location; (ii) post notice of restricted access to paper records; and (iii) utilize an access log or sign-in sheet to record access to paper records.

5) The District shall implement safeguards required by the Criminal Justice Information Services (CJIS) Security Policy for CJI maintained in electronic format, including, but not limited to, the following procedures: (i) maintain CJI on secure electronic systems and media; (ii) position information systems in such a way as to prevent unauthorized individuals from accessing and viewing CJI; (iii) store electronic media containing CJI in a secure location; (iv) instituting access controls to limit access to Permitted Individual; (v) validate and authenticate information system users accessing CJI; (vi) develop protocols for configuration management and providing necessary access for system modifications and maintenance; (vii) provide the capability to detect and protect against threats to the integrity of CJI; (viii) develop parameters (including time stamps) for auditing electronic systems containing CJI; and (ix) institute media protection policies and procedures.

6) The District shall not allow personally-owned information systems, such as flash drives, DVDs, CDs, tablets, mobile devices, laptops, or air cards to access, process, store, or transmit CJI.

7) The District shall not allow remote access to CJI.

F. Disclosure of Criminal Justice Information

1) Permitted Individuals may disclose CJI as follows:

(i) to District employees or staff upon prior written approval of the Superintendent, CJI Officer or their designees when, in their reasonable discretion, such disclosure is reasonably necessary for the performance of District function or policy and is consistent with applicable law;

(ii) to third-party individuals or entities, including but not limited to advisors, attorneys and electronic and hard copy record and storage companies (each a "Recipient") when such disclosure has been approved by the Superintendent, CJI Officer or their designees, and is consistent with applicable law; and

(iii) as required or otherwise permitted by law.

2) The District shall log each instance in which CJI is disclosed pursuant to these regulations.

G. Security Incident Response.

1) For purposes of these regulations, "Security Incident" means the actual or suspected acquisition, access, use, or disclosure of CJI in a manner not permitted by these regulations or applicable law.

2) District employees and staff must immediately report a Security Incident to the CJI Officer.

3) The CJI Officer shall investigate, collect relevant evidence and respond to all Security Incidents.

4) The CJI Officer will document each Security Incident, including, but not limited to, the details of the Security Incident, the District's response, the outcome, steps taken to mitigate harm to affected individuals, and any changes to District policies or security procedures to avoid reoccurrence of the Security Incident.

5) The District shall require in writing any Recipients to report to the District any Security Incidents without unreasonable delay after discovery of a Security Incident. The Recipient's notice to the District shall include: (a) the identification of each individual whose CJI has been, or is reasonably believed by the Recipient to have been, accessed, acquired, or disclosed during the Security Incident; and (b) other available information that the District reasonably requests with respect to its investigation or that the District is required to include in notifications to affected individuals or governmental agencies. The Recipient shall promptly update its original notice to the District as additional information becomes available.

6) The District shall notify affected individuals and/or appropriate government agencies to the extent required by law or as otherwise determined appropriate by the District in its reasonable discretion.

H. Auditing

1) The District shall implement audit and accountability controls to increase the probability of Permitted Individuals conforming to the requirements of these regulations and applicable law. At a minimum, the auditing and accountability controls shall generate sufficient information to establish, with respect to the access, use or dissemination of CJI, what events occurred, the sources of the events and the outcome of the events.

2) The CJI Officer shall review audit reports at least weekly. Audit reports that indicate potential inappropriate activity shall be investigated as a Security Incident in accordance with these regulations.

3) Annually, the District shall review Permitted Individual's accounts to ensure that access and account privileges are commensurate with job functions, need-to-now, and employment status.

I. Record Retention

1) The District shall maintain CJI consistent with current record retention laws. Records containing CJI shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

2) The District shall maintain audit records and any transaction logs for at least one year.

3) The District shall destroy all records containing CJI when the District is no longer required to keep CJI on file.

I. Disposal and Destruction of CJI

1) For paper records containing CJI, destroyed means the records shall be disposed of in a manner that makes the CJI unreadable, indecipherable, and otherwise unable to be reconstructed, including but not limited to shredding or incinerating the records.

2) For electronic media containing CJI, destroyed means the records shall be disposed of or wiped of CJI using one of the following methods: (a) sanitize (electronically overwrite the media with non-sensitive data at least three times), (b) purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or (c) for inoperable media, destroying the media (disintegration, pulverization, melting, incinerating, or shredding). In each instance, the method used shall render the CJI unreadable, indecipherable, and otherwise unable to be reconstructed.

3) The destruction of media pursuant to this Section shall be witnessed or carried out only by authorized personnel.

4.) The District shall document the destruction of media pursuant to this Section and the method by which the media was destroyed.

J. Training

1) The District shall provide awareness training and education on these regulations and the use, disclosure and safeguarding of CJI to all District employees and staff persons with access to CJI, in accordance with then-current District training and education policies and procedures, provided that such training shall be provided within six (6) months of initial engagement and no less than biennially thereafter. The District shall document the provision of all training and education provided hereunder.

2) The training shall address those topics required by then-current law or regulatory guidance.

K. Sanctions

Violations of these regulations shall be investigated by the District and may result in discipline or sanctions, up to and including termination of employment, all in accordance with then-current District policies and procedures and applicable collective bargaining rights and obligations.

Legal References:

Conn. Gen. Stat. 10-221d

28 CFR § 20.1 *et seq.*

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, United States Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

ADOPTED: March 21, 2017

WESTON PUBLIC SCHOOLS
Weston, Connecticut