Administrative Regulation

CRIMINAL HISTORY RECORDS CHECK

A. A criminal history records check will be completed for all current and proposed employees that are temporary, regular full or part-time staff, substitutes, appropriate performance contractors and anyone else who is assigned to regularly and continuously work under contract to provide instructional or administrative services to students. All criminal history record check reports received from the State Police or produced by the State Police and received by the District from another proper source, will be maintained in separate digital files.

1. All employees must complete a conviction disclosure form.

2. The individual's name, identification numbers (social security/driver's license) and fingerprints will be submitted to the State Police Central Records Division and the FBI for processing the records check.

3. No individual shall be employed until receipt and review of his/her criminal history check.

4. Ingham ISD will neither retain nor employ any individual who has been convicted of any of the listed offenses, whether felony or misdemeanor as defined in Section 2 of the Sex Offenders Registration Act 1994 PA 295, MCLA 28.722.

B. Use of Prior Criminal History Records Check (CHRC)

1. For substitute teachers currently working in another district, public school academy or non-public school in the state, the Superintendent may use a report received from the State Police by such school to confirm that the individual has no criminal history. Absent such confirmation, a criminal history record check shall be performed.

2. Individuals working in multiple districts may authorize the release of a prior criminal history records check with another district in lieu of an additional check for either direct employment or working regularly and consistently under contract in the schools.

3. Individuals who previously received a statutorily required criminal background check and who have been continuously employed by a school district, intermediate school district, public school academy or non-public school within the state, with no separation, may have their previous record check sent to the District in lieu of submitting to a new criminal background check. If this method is used, the Director of Human Resources must confirm that the record belongs to that individual and whether there have been any additional convictions by processing the individual's name, sex and date of birth through the Internet Criminal History Access Tool (ICHAT).

4. "No separation," for purposes of the preceding paragraph, means a lay off or leave of absence of less than twelve (12) months with the same employer; or the employee transfers without a break in service to another school district, intermediate school district, public school academy or non-public school within the state.

C. Procedures regarding findings on criminal history records other than "listed offenses"

1. If a felony conviction is indicated on the records check, this information will be brought immediately to the Superintendent's attention by the Director of Human Resources. The Superintendent shall inform the Board of the felony conviction and place the matter on the board agenda, if the conviction involves a current staff member or an individual who is being recommended for hire. (See also 6289.00-R(3)

2. Record checks for all other individuals who are deemed to be regularly and continuously under contract with the District shall be dealt with as required by law.

3. Misdemeanor convictions other than those detailed as "listed offenses" will be reviewed by the Director of Human Resources or brought to the Superintendent's attention where appropriate.

D. Authoritative knowledge of a conviction

1. If the Superintendent or Board President is notified or learns from an authoritative source that a person holding state board approval has been convicted of a felony or is on the "listed offenses," they will seek to verify the information first, but shall notify the State Superintendent of the conviction within 15 days after learning of the conviction.

2. If a school official has notice from an authoritative source that an individual has been convicted of a listed offense, the District shall not employ that individual in any capacity or allow that person to regularly and continuously work under contract.

E. Employee charged with a crime:

1. The employee shall report to the Michigan Department of Education and the District within three (3) business days if charged with an offense listed under MCL 380.1535A(1).

F. When an employee is convicted of a crime:

1. The employee shall immediately notify the court that he or she is employed by the District, if the employee is convicted of a felony or an offense listed in MCL 380.1535a(1). The employee shall provide a notification form to the Prosecuting Attorney, Superintendent of Public Instruction, and the Superintendent of the school district. (MCL 380.1230D)

2. A conviction of a crime listed in MCL 380.1535a(1), or failure to report being charged or convicted with a crime, is considered reasonably and adversely related to the ability of the person to serve in an elementary or secondary school and is sufficient grounds to support a discharge or demotion of a teacher on continuing tenure. (MCL 38.101a)

3. If a teacher is convicted of a felony that is not a listed offense or a misdemeanor that is a listed offense, the Board may discontinue the teacher's salary upon the date of conviction. (MCL 38.103)

4. If a teacher is convicted of a felony that is a listed offense, the Board shall discontinue the teacher's salary upon date of conviction or learning of a conviction, whichever occurs later. (MCL 38.103)

5. If a District receives a report from the state police disclosing that an individual has been convicted of a felony that is a listed offense, the District shall not employ the individual in any capacity or allow the individual to regularly and continuously work in any of its schools. (MCL 380.1230)

6. If a District receives a report from the state police disclosing that an individual has been convicted of a felony that is not a listed offense, the District shall not employ the individual in any capacity or allow the individual to regularly and continuously work in any of its schools, unless the Superintendent of the district and the Board specifically approve the employment or work assignment in writing. (MCL 380.1230)

7. If the Board has notice from an authoritative source that an individual has been convicted of a listed offense, the Board shall not employ the individual in any capacity, and shall not allow the individual to regularly and continuously work under contract with any of its schools. (MCL 380.1230c)

8. If a teacher enters a plea of guilty or no contest or is convicted of a crime listed in MCL 380.1535a(2), the District shall not pay any wages to that teacher. Instead, the District shall discontinue the teacher's salary until the Superintendent of Public Instruction makes a final determination of whether or not to suspend or revoke the person's teaching certificate. If the certificate is suspended or revoked, the teacher forfeits the wages being withheld. But if the certificate is not suspended or revoked, the teacher shall be paid the wages withheld without interest. (MCL 1535a(4)

G. Volunteers working directly with students shall go through a background check. Their driver's license number and name shall be sent to the state police for review through the internet criminal history access tool (ICHAT). If any record returns, the appropriate action will be taken as earlier detailed.

H. Confidentiality

1. All information and records obtained from such criminal background inquiries and disclosures are to be considered confidential and shall not be released or disseminated to those not directly involved in evaluating the applicant's qualifications. Records involving misdemeanor convictions for sexual or physical abuse or any felony are not subject to these restrictions. Violation of confidentiality is considered a misdemeanor with fines up to $10,000.

2. Any notification received from the Michigan Department of Education or Michigan State Police regarding District employees with criminal convictions shall be exempt from disclosure under the Freedom of Information Act (FOIA) for the first fifteen (15) days until the accuracy of the information can be verified. Thereafter, only information about felony convictions or misdemeanor convictions involving physical or sexual abuse may be disclosed in reference to a Freedom of Information Act request.

3. Criminal history reports may be released with the written authorization of the individual.

I. Media Protection – Access to digital and physical media in all forms, which contains Criminal History Record Information (CHRI) provided by the MSP through the statutory record check process, is restricted to authorized individuals only.

1. Media Storage and Access – All digital and physical media shall be stored in a physically secure and controlled area, such as locked office, locked cabinet or other similarly secure area(s) which can only be accessed by authorized individuals. If such security cannot be reasonably provided, then all digital CHRI background data shall be encrypted.

2. Media Transport – Should the need arise to move CHRI media outside of the secured location or controlled area, the Ingham Intermediate School District shall establish and implement appropriate security controls to prevent compromise of the data while transporting. The transport of CHRI media will be conducted by authorized personnel. CHRI media includes:

   a. Physical CHRI media such as paper/hard copies.
   b. Digital CHRI media such as laptops; computer hard drives; and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card(s).

   The specific steps of how agency transport will occur:

   a. The Local Agency Security Office (LASO) or another authorized individual will handle and transport CHRI media.
   b. A transport would only occur if a rare event happened that required movement of CHRI media outside of the controlled area. This would be approved by the LASO.
   c. A locked container would be used to move to transport the media.
   d. The media being transported would remain in the physical possession of the designated authorized employee until CHRI media is delivered to its intended destination.

3. Digital Media Disposal/Sanitization – Without ensuring the proper disposal of installed and removable digital storage, information security risks can be created by reassigning, surplussing, transferring, trading-in, disposing of computers, or replacing digital storage media and computer software. Therefore, once digital CHRI media devices are determined no longer needed by the agency, devices shall be sanitized and disposed of according to the most current FBI CJIS Security Policy. Due to the presence of temporary files (data remanence), devices where digital media was once stored, processed, and/or used for dissemination (fax, scanners, computers, laptops, etc.) shall be sanitized in a manner that gives assurance that the information cannot be recovered prior to disposal of or upon the reassigning or recycling of such devices. An "erase" feature (e.g., putting a document in a “trash can” icon) or deleting a file is not sufficient for sensitive information, because the information may still be recoverable. The agency will provide steps for the sanitization and disposal of devices where CHRI media was once stored, processed, and/or used.

   Ingham ISD does not store information digitally.

4. Disposal of Physical Media

   Once physical CHRI media (paper copies) is determined no longer needed by the agency, media shall be destroyed and disposed of according to the FBI CJIS Security Policy. Formal procedures for the secure disposal or destruction of physical media:

The specific steps of how disposal of physical media will occur:

a. Ingham ISD does not actively store physical media. It is destroyed once the information is scanned into a stand-alone laptop.
b. The disposal or destruction of physical CHRI media shall be witnessed or carried out by an authorized user.
c. Crosscut shredding is used as the method of destruction.

J. Auditing and Accountability

The District's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. In the even the District does not use an automated system, manual recording of activities shall still take place.

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.

2. Successful and unsuccessful attempts to:
    a. Access permission on a user account, file, directory or other system resource;
    b. Create permission on a user account, file, directory, or other system resource;
    c. Write permission on a user account, file directory or other system resource;
    d. Delete permission on a user account, file, directory or other system resource;
    e. Change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change accounts passwords.

4. Successful and unsuccessful actions by privileged accounts.

5. Successful and unsuccessful attempts for users to:

    a. Access the audit log file;

    b. Modify the audit log file;

    c. Destroy the audit log file.

The following content shall be included with every audited event: 1) date and time of the event; 2) the component of the information system (e.g., software component, hardware component) where the even occurred; 3) type of event; 4) user identity; and 5) outcome (success or failure) of the event.

Audit Monitoring, Analysis and Reporting – The District shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, to investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week, and should be increased if volume indicates an elevated need for audit review.

Time Stamps – The District's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records.

Protection of Audit Information – The District's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

Audit Record Retention – The District shall retain audit records for at least on (1) year. Once the minimum retention time period has passed, the District may continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.

LEGAL CITATION: MCLA 380.1535, 380.1230, 38.101, 38.103
ADMINISTRATIVE REGULATION

Approved: June 18, 1991
Amended: May 2, 2006
March 10, 2014
January 26, 2017
January 25, 2019