NEW POLICY - VOL. 32, NO. 1

CRIMINAL HISTORY RECORD CHECK

Before the District hires any employee (full or part-time) or allows any individual under contract to continuously and regularly work in the schools, a criminal history records check shall be conducted in accordance with State law.

"Under contract" shall apply to individuals, as well as owners and employees of entities, who contract directly with the District or with a third party vendor, management company, or similar contracting entity to provide food, custodial, transportation, counseling or administrative services on more than an intermittent or sporadic basis. It shall also apply to individuals or entities providing instructional services to students or related auxiliary services to special education students.

Prior to allowing an individual, who is subject to the criminal history record check requirement, to work in the District, the District shall submit a fingerprint-based check on the individual, using Michigan State Police (MSP) Form RI-030 (7/2012), regardless of whether the individual will work directly for the District or be contracted through a third-party vendor, management company or similar contracting entity ("Private Contractors"). Except as provided below, the report from the MSP must be received, reviewed and approved by the District prior to the individual commencing work.

Such Private Contractors cannot receive or retain criminal history record information ("CHRI").[1] Where the District will contract with a Private Contractor for the services of an individual, the District will notify the Private Contractor(s), after review of the MSP report, whether the individual has been approved to work within the District. The District may not give any details, including the fact that a criminal history check was run. Notice for approval to work in the District should use the Affidavit of Assignment or similar "red light/green light" procedure.

Should it be necessary to employ a person or contract for a person to maintain continuity of the program prior to receipt of the criminal history report, the Superintendent may contract on a provisional basis until the report is received. Any such provisional hire requires that:

A. the record check has been requested;

B. the applicant has signed a disclosure of all convictions and acknowledges that employment may be terminated if there are discrepancies; and

C. the hiring occurs during the school year or not more than thirty (30) days before the beginning of the school year.

---

[1] Individuals who submit and receive such criminal history record checks on behalf of the District must be direct employees of the District. Notwithstanding this, Information Technology contractors and vendors may be granted access to CHRI subject to successful completion of a national fingerprint-based criminal history record check as detailed in Policy 8321.

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.

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 Superintendent 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).

"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.

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 the individual's confidential file, which must be maintained in compliance with Policy 8321 and AG 8321.

When the District receives a report that shows an individual has been convicted of a listed offense under State statutes or any felony, the Superintendent shall take steps to verify that information using public records, in accordance with the procedures provided by the State Department of Education.

Verified convictions may result in termination of employment or rejection of an application. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of a "listed" offense as defined in M.C.L. 28.722. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of any felony unless both the Superintendent and the Board provide written approval.

The District must report as directed by and to the State Department of Education the verified information regarding conviction for any listed offense or conviction for any felony and the action taken by the District with regard to such conviction. Such report shall be filed within sixty (60) days of receipt of the original report of the conviction.

The Superintendent shall establish the necessary procedures for obtaining from the Criminal Records Division of the State Police any criminal history on the applicant maintained by the State Police. In addition, the Superintendent shall request the State Police to obtain a criminal history records check from the Federal Bureau of Investigation.

An applicant must

(X) submit, at no expense to the District,

or

( ) provide, at the District's expense,

a set of fingerprints, prepared by an entity approved by the Michigan State Police, as part of his/her employment application or as required by State law for continued employment. **In the case of difficult-to-fill positions, the Superintendent may opt to provide fingerprints at the District's expense.**

Confidentiality

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 who have not been given access to CHRI by the Superintendent Violation of confidentiality is considered a misdemeanor punishable by a fine up to $10,000.

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 FOIA request.

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

Records may also be released, in accordance with statute, upon the request of a school district, intermediate school district, public school academy or non-public school when the individual is an applicant for employment at such school and there has been no separation from service, as defined in this policy and by statute.

M.C.L. 380.1230 et. seq., 380.1535, 380.1535a, 380.1809, 28.722

REVISED POLICY - VOL. 32, NO. 1

CRIMINAL HISTORY RECORD CHECK

Before the District hires any employee (full or part-time) or allows any individual under contract to continuously and regularly work in the schools, a criminal history records check shall be conducted in accordance with State law.

"Under contract" shall apply to individuals, as well as owners and employees of entities, who contract directly with the District or with a third party vendor, management company, or similar contracting entity to provide food, custodial, transportation, counseling or administrative services on more than an intermittent or sporadic basis. It shall also apply to individuals or entities providing instructional services to students or related auxiliary services to special education students.

Prior to allowing an individual, who is subject to the criminal history record check requirement, to work in the District, the District shall submit a fingerprint-based check on the individual, using Michigan State Police (MSP) Form RI-030 (7/2012), regardless of whether the individual will work directly for the District or be contracted through a third-party vendor, management company or similar contracting entity ("Private Contractors"). Except as provided below, the report from the MSP must be received, reviewed and approved by the District prior to the individual commencing work.

Such Private Contractors cannot receive or retain criminal history record information ("CHRI").[1] Where the District will contract with a Private Contractor for the services of an individual, the District will notify the Private Contractor(s), after review of the MSP report, whether the individual has been approved to work within the District. The District may not give any details, including the fact that a criminal history check was run. Notice for approval to work in the District should use the Affidavit of Assignment or similar "red light/green light" procedure.

Should it be necessary to employ a person or contract for a person to maintain continuity of the program prior to receipt of the criminal history report, the Superintendent may contract on a provisional basis until the report is received. Any such provisional hire requires that:

A. the record check has been requested;

B. the applicant has signed a disclosure of all convictions and acknowledges that employment may be terminated if there are discrepancies; and

C. the hiring occurs during the school year or not more than thirty (30) days before the beginning of the school year.

For substitute teachers or substitute bus drivers 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 the individual has no criminal history. Absent such confirmation, a criminal history record check shall be performed.

---

[1] Individuals who submit and receive such criminal history record checks on behalf of the District must be direct employees of the District. Notwithstanding this, Information Technology contractors and vendors may be granted access to CHRI subject to successful completion of a national fingerprint-based criminal history record check as detailed in Policy 8321.

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.

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 Superintendent 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).

"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.

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 the individual's confidential file, which must be maintained in compliance with Policy 8321 and AG 8321.

When the District receives a report that shows an individual has been convicted of a listed offense under State statutes or any felony, the Superintendent shall take steps to verify that information using public records, in accordance with the procedures provided by the State Department of Education.

Verified convictions may result in termination of employment or rejection of an application. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of a "listed" offense as defined in M.C.L. 28.722. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of any felony unless both the Superintendent and the Board provide written approval.

The District must report as directed by and to the State Department of Education the verified information regarding conviction for any listed offense or conviction for any felony and the action taken by the District with regard to such conviction. Such report shall be filed within sixty (60) days of receipt of the original report of the conviction.

The Superintendent shall establish the necessary procedures for obtaining from the Criminal Records Division of the State Police any criminal history on the applicant maintained by the State Police. In addition, the Superintendent shall request the State Police to obtain a criminal history records check from the Federal Bureau of Investigation.

An applicant must

(X) submit, at no expense to the District,

or

( ) provide, at the District's expense,

a set of fingerprints, prepared by an entity approved by the Michigan State Police, as part of his/her employment application or as required by State law for continued employment. **In the case of difficult-to-fill positions, the Superintendent may opt to provide fingerprints at the District's expense.**

Confidentiality

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 who have not been given access to CHRI by the Superintendent Violation of confidentiality is considered a misdemeanor punishable by a fine up to $10,000.

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 FOIA request.

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

Records may also be released, in accordance with statute, upon the request of a school district, intermediate school district, public school academy or non-public school when the individual is an applicant for employment at such school and there has been no separation from service, as defined in this policy and by statute.

M.C.L. 380.1230 et. seq., 380.1535, 380.1535a, 380.1809, 28.722

REVISED POLICY - VOL. 32, NO. 1

CRIMINAL HISTORY RECORD CHECK

Before the District hires any employee (full or part-time) or allows any individual under contract to continuously and regularly work in the schools, a criminal history records check shall be conducted in accordance with State law.

"Under contract" shall apply to individuals, as well as owners and employees of entities, who contract directly with the District or with a third-party vendor, management company, or similar contracting entity, to provide food, custodial, transportation, counseling or administrative services on more than an intermittent or sporadic basis. It shall also apply to individuals or entities providing instructional services to students or related auxiliary services to special education students.

Prior to allowing an individual, who is subject to the criminal history record check requirement, to work in the District, the District shall submit a fingerprint-based check on the individual, using Michigan State Police (MSP) Form RI-030 (7/2012), regardless of whether the individual will work directly for the District or be contracted through a third-party vendor, management company or similar contracting entity ("Private Contractors"). Except as provided below, the report from the MSP must be received, reviewed and approved by the District prior the individual commencing work.

Such Private Contractor(s) cannot receive or retain criminal history record information ("CHRI").[1] Where the District will contract with a Private Contractor for the services of an individual, the District will notify the Private Contractor(s), after review of the MSP report, whether the individual has been approved to work within the District. The District may not give any details, including the fact that a criminal history check was run. Notice for approval to work in the District should use the Affidavit of Assignment or similar "red light/green light" procedure.

Should it be necessary to employ a person or contract for a person to maintain continuity of the program prior to receipt of the criminal history report, the Superintendent may contract on a provisional basis until the report is received. Any such provisional hire requires that:

A. the record check has been requested;

B. the applicant has signed a disclosure of all convictions and acknowledges that employment may be terminated if there are discrepancies; and

C. the hiring occurs during the school year or not more than thirty (30) days before the beginning of the school year.

---

[1] Individuals who submit and receive such criminal history record checks on behalf of the District must be direct employees of the District. Notwithstanding this, Information Technology contractors and vendors may be granted access to CHRI subject to successful completion of a national fingerprint-based criminal history record check as detailed in Policy 8321.

Such an inquiry shall also be made for regular substitutes who may be employed by the District. A substitute support staff person shall be required to submit to a criminal history records check if they work more than _____ **hours** per week in the schools, on a regular and consistent basis, even if such work is only as needed.

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.

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 Superintendent 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).

"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.

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 the individual's confidential file, which must be maintained in compliance with Policy 8321 and AG 8321.

When the District receives a report that shows an individual has been convicted of a listed offense under State statutes or any felony, the Superintendent shall take steps to verify that information using public records, in accordance with the procedures provided by the State Department of Education.

Verified convictions may result in termination of employment or rejection of an application. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of a "listed" offense as defined in M.C.L. 28.722. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of any felony unless both the Superintendent and the Board provide written approval.

The District must report as directed by and to the State Department of Education the verified information regarding conviction for any listed offense or conviction for any felony and the action taken by the District with regard to such conviction. Such report shall be filed within sixty (60) days of receipt of the original report of the conviction.

The Superintendent shall establish the necessary procedures for obtaining from the Criminal Records Division of the State Police any criminal history on the applicant maintained by the State Police. In addition, the Superintendent shall request the State Police to obtain a criminal history records check from the Federal Bureau of Investigation.

An applicant must

(X) submit, at no expense to the District,

or

( ) provide, at the District's expense,

a set of fingerprints, prepared by an entity approved by the Michigan State Police, as part of his/her employment application or as required by State law for continued employment. **In the case of difficult-to-fill positions, the Superintendent may opt to provide fingerprints at the District's expense.**

Confidentiality

All information and records obtained from such inquiries and disclosures are to be considered confidential and shall not be released or disseminated to those who have not been given access to CHRI by the Superintendent. Violation of confidentiality is considered a misdemeanor punishable by a fine up to $10,000.

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 FOIA request.

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

Records may also be released, in accordance with statute, upon the request of a school district, intermediate school district, public school academy or non-public school when the individual is an applicant for employment at such school and there has been no separation from service, as defined in this policy and by statute.

M.C.L. 380.1230 et seq., 380.1535, 380.1535a, 380.1809, 28.722

REVISED POLICY - VOL. 32, NO. 1

CRIMINAL HISTORY RECORD CHECK

Before the District hires any employee (full or part-time) or allows any individual under contract to continuously and regularly work in the schools, a criminal history records check shall be conducted in accordance with State law.

"Under contract" shall apply to individuals, as well as owners and employees of entities, who contract directly with the District or with a third-party vendor, management company, or similar contracting entity, to provide food, custodial, transportation, counseling or administrative services on more than an intermittent or sporadic basis. It shall also apply to individuals or entities providing instructional services to students or related auxiliary services to special education students.

Prior to allowing an individual, who is subject to the criminal history record check requirement, to work in the District, the District shall submit a fingerprint-based check on the individual, using Michigan State Police (MSP) Form RI-030 (7/2012), regardless of whether the individual will work directly for the District or be contracted through a third-party vendor, management company or similar contracting entity ("Private Contractors"). Except as provided below, the report from the MSP must be received, reviewed and approved by the District prior to the individual commencing work.

Such Private Contractors cannot receive or retain criminal history record information ("CHRI").[1] Where the District will contract with a Private Contractor for the services of an individual, the District shall notify the Private Contractor(s), after review of the MSP report, whether the individual has been approved to work within the District. The District may not give any details, including the fact that a criminal history check was run. Notice for approval to work in the District should use the Affidavit of Assignment or similar "red light/green light" procedure.

---

[1] Individuals who act on behalf of the District, work on a regular or continuous basis in the District, are involved in the hiring process of District employees, and have successfully undergone a fingerprint-based criminal history record check by the District, may continue to submit and receive such criminal history record checks on behalf of the District, regardless of their status as employees, contractors, vendors or similar classification.

Should it be necessary to employ a person or contract for a person to maintain continuity of the program prior to receipt of the criminal history report, the Superintendent may contract on a provisional basis until the report is received. Any such provisional hire requires that:

A. the record check has been requested;

B. the applicant has signed a disclosure of all convictions and acknowledges that employment may be terminated if there are discrepancies; and

C. the hiring occurs during the school year or not more than thirty (30) days before the beginning of the school year.

For substitute teachers or substitute bus drivers 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 the individual has no criminal history. Absent such confirmation, a criminal history record check shall be performed.

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.

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 Superintendent 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).

"No separation," for purposes of the preceding paragraph, means a layoff 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.

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 the individual's confidential file, which must be maintained in compliance with Policy 8321 and AG 8321.

When the District receives a report that shows an individual has been convicted of a listed offense under state statutes or any felony, the Superintendent shall take steps to verify that information using public records, in accordance with the procedures provided by the State Department of Education.

Verified convictions may result in termination of employment or rejection of an application. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of a "listed" offense as defined in M.C.L. 28.722. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of any felony unless both the Superintendent and the Board provide written approval.

The District must report as directed by and to the State Department of Education the verified information regarding conviction for any listed offense or conviction for any felony and the action taken by the District with regard to such conviction. Such report shall be filed within sixty (60) days or receipt of the original report of the conviction.

The Superintendent shall establish the necessary procedures for obtaining from the Criminal Records Division of the State Police any criminal history on the applicant maintained by the State Police. In addition, the Superintendent shall request the State Police to obtain a criminal history records check from the Federal Bureau of Investigation.

An applicant must

(X) submit, at no expense to the District,

or

( ) provide, at the District's expense,

a set of fingerprints, prepared by an entity approved by the Michigan State Police, upon receiving an offer of employment, or as required by State law for continued employment. **In the case of difficult-to-fill positions, the Superintendent may opt to provide fingerprints at the District's expense.**

Confidentiality

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 punishable by a fine up to $10,000.

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 FOIA request.

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

Records may also be released, in accordance with statute, upon the request of a school district, intermediate school district, public school academy or non-public school when the individual is an applicant for employment at such school and there has been no separation from service, as defined in this policy and by statute.

M.C.L. 380.1230 et. seq., 380.1535, 380.1535a, 380.1809, 28.722

REVISED POLICY - VOL. 32, NO. 1

CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY)

The District is required by State law to have the Michigan State Police (MSP) obtain both a State and a Federal Bureau of Investigation (FBI) criminal history record information (CHRI) background check report for all employees of the District and contractors, vendors and their employees who work on a regular and continuous basis in the District. To assure the security, confidentiality, and integrity of the CHRI background check information received from the MSP/FBI, the following standards are established:

A. Sanctions for Non-Compliance

Employees who fail to comply with this policy and any guidelines issued to implement this policy will be subject to discipline for such violations. Discipline will range from counseling and retraining to discharge, based on the nature and severity of the violation. All violations will be recorded in writing, with the corrective action taken. The Superintendent shall review, approve, sign and date all such corrective actions.

B. Local Agency Security Officer (LASO)

The **Executive Director of Human Resources** shall be designated as the District's Security Officer and shall be responsible for overall implementation of this policy and for data and system security. This shall include:

1. ensuring that personnel security screening procedures are being followed as set forth in this policy;

2. ensuring that approved and appropriate security measures are in place and working as expected;

3. supporting policy compliance and instituting the incident response reporting procedures;

4. ensuring that the Michigan State Police are promptly informed of any security incidents involving the abuse or breach of the system and/or access to criminal justice information;

5. to the extent applicable, identifying and documenting how District equipment is connected to the Michigan State Police system;

6. to the extent applicable, identify who is using the Michigan State Police approved hardware, software and firmware, and ensuring that no unauthorized individuals have access to these items.

The District's LASO shall be designated on the appropriate form as prescribed and maintained by the Michigan State Police. A new form shall be submitted every time a new LASO is designated.

C. Agency User Agreements

The District shall enter into any required User Agreement for Release of CHRI ("User Agreement"), and future amendments, by the Michigan State Police necessary to access the required CHRI on applicants, volunteers, and all other statutorily required individuals, such as contractors and vendors and their employees assigned to the District. The LASO shall be responsible for the District's compliance with the terms of any such User Agreement.

D. Personnel Security

All individuals that require access to any criminal justice information shall be subject to the following standards prior to granting of access:

1. Background Checks - A Michigan (or state of residency if other than Michigan) and a national fingerprint-based criminal history record check shall be conducted within thirty (30) days of assignment to a position with direct access to criminal justice information or with direct responsibility to configure and maintain computer systems and networks with direct access to criminal justice information.

    a. A felony conviction of any kind will disqualify an individual for access to criminal justice information.

    b. If any other results/records are returned, the individual shall not be granted access until the LASO reviews and determines access is appropriate. This includes, but is not limited to, any record which indicates the individual may be a fugitive or shows arrests without convictions. Such approval shall be recorded in writing, signed, dated and maintained with the individual's file.

c. If support personnel, contractors or custodial workers need to be in an area where CHRI is maintained or processed, they shall be escorted by or under the supervision of authorized personnel at all times while in those area. Information Technology contractors or vendors will be physically or virtually escorted by authorized personnel anytime said individual have access to facilities, areas, rooms, or an agency's CHRI information system.

2. Subsequent Arrest/Conviction - If an individual granted access to criminal justice information is subsequently arrested and/or convicted, access shall be suspended immediately until the matter is reviewed by the LASO to determine if continued access is appropriate. Such determination shall be recorded in writing, signed, dated and maintained with the individual's file. In the event that the LASO has the arrest/conviction, the Superintendent (if not the designated LASO) shall make the determination. If the Superintendent is also the designated LASO, the determination shall be made by Executive Director of Human Resources. Except that, as noted in D(1)(a), individuals with a felony conviction of any kind will have their access indefinitely suspended.

3. Public Interest Denial - If the LASO determines that access to criminal justice information by any individual would not be in the public interest, access shall be denied whether that person is seeking access or has previously been granted access. Such decision and reasons shall be in writing, signed, dated and maintained in the individual's file.

4. Approval for Access - All requests for access to criminal justice information shall be as specified and approved by the LASO. Any such designee must be a direct employee of the District. The District must maintain a readily accessible list that includes the names of all LASO approved personnel with access to criminal justice information, as well as the reason for providing each individual access. This list shall be made available to Michigan State Police upon request.

5. Termination of Employment/Access – Within twenty-four (24) hours of the termination of employment, all access to criminal justice information shall be terminated immediately for that individual, such as closing the individual's account and/or blocking access to any systems containing such information at the District.

6. Transfer/Re-assignment - When an individual who has been granted access to criminal justice information has been transferred or re-assigned to other duties, the LASO shall determine whether continued access is necessary and appropriate. If not, s/he shall take such steps as necessary to block further access to such information within the twenty-four (24) hour period immediately following the transfer or reassignment.

7. Information Technology Contractors and Vendors[1] – Prior to granting access to criminal justice information to an IT contractor or vendor, identification must be verified via a Michigan (or state of residency if other than Michigan) and national fingerprint-based criminal history record check. A felony conviction of any kind, as well as any outstanding arrest warrant, will disqualify an IT contractor or vendor for access to criminal justice information. A contractor or vendor with a criminal record of any other kind may be granted access if the LASO determines the nature or severity of the misdemeanor offense(s) does not warrant disqualification. If any other results/records are returned, the individual shall not be granted access until the LASO reviews and determines access is appropriate.

E. Media Protection

Access to digital and physical media in all forms, which contains criminal history background information provided by the Michigan State Police through the statutory record check process, is restricted to authorized individuals only. Only individuals involved in the hiring determination of both District employees and volunteers shall be authorized to access digital and physical media containing CHRI.

1. Media Storage and Access – All digital and physical media shall be stored in a physically secure location or 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. Digital media shall be stored on a District or School server. Storage on a third party server, such as cloud service, is not permitted. Storage of digital media must conform to the requirements in AG 8321.

[1]Non-Information Technology contractors or vendors shall not have access to criminal justice information.

2. Media Transport – Digital and physical media shall only be transported upon sufficient justification approved by the LASO. Digital and physical medial shall be protected when being transported outside of a controlled area. Only authorized individuals shall transport the media. Physical media (e.g. printed documents, printed imagery, etc.) shall be transported using a locked container, sealed envelope, or other similarly secure measure. To the extent possible, digital media (e.g., hard drives and removable storage devices such as disks, tapes, flash drives and memory cards) shall be either encrypted and/or be password protected during the transport process. The media shall be directly delivered to the intended person or destination and shall remain in the physical control and custody of the authorized individual at all times during transport. Access shall only be allowed to an authorized individual.

3. Media Disposal/Sanitization – When the CHRI background check is no longer needed, the media upon which it is stored shall either be destroyed or sanitized. The LASO and the Superintendent shall approve in writing the media to be affected. This record shall be maintained by the LASO for a period of at least five (5) years. **[Note: the regulations do not specify a specific period for maintaining this information. This time period is suggested as it will likely cover most statutes of limitation and can be retained in digital format.]**

   a. Digital Media - Sanitization of the media and deletion of the data shall be accomplished by either overwriting at least three (3) times or by degaussing, prior to disposal or reuse of the media. If the media is inoperable or will not be reused, it shall be destroyed by shredding, cutting, or other suitable method to assure that any data will not be retrievable.

   b. Physical Media – Disposal of documents, images or other type of physical record of the criminal history information shall be cross-cut shredded or incinerated. Physical security of the documents and their information shall be maintained during the process by authorized individuals. Documents may not be placed in a waste basket or burn bag for unauthorized individuals to later collect and dispose of.

   All disposal/sanitization shall be either conducted or witnessed by authorized personnel to assure that there is no misappropriation of, or unauthorized access to, the data to be deleted. Written documentation of the steps taken to sanitize or destroy the media shall be maintained for ten (10) years, and must include the date as well as the signatures of the person(s) performing and/or witnessing the process. (See also, AG 8321.)

4. Mobile Devices – A personally owned mobile device (mobile phone, tablet, laptop, etc.) shall not be authorized to access, process, store or transmit criminal justice information unless the District has established and documented the specific terms and conditions for personally owned mobile devices.

F. CHRI Background Check Consent and Documentation

All individuals requested to complete a fingerprint-based CHRI background check must have given written consent-properly signed and dated—at time of application and be notified fingerprints will be used to check the criminal history records of the FBI, prior to completing a fingerprint-based CHRI background check. The most current and unaltered Livescan form (RI-030) will satisfy this requirement and must be retained. Individuals subject to a fingerprint-based CHRI background check shall be provided the opportunity to complete or challenge the accuracy of the individual's criminal history record.

Some type of documentation identifying the position for which a fingerprint-based CHRI background check has been obtained must be retained for every CHRI background check conducted, such as an offer letter, employment agreement, new hire checklist, employment contract, volunteer background check form, etc.

G. Controlled Area/Physical Protection

All CHRI obtained from the Michigan State Police pursuant to the statutorily required background checks shall be maintained in a physically secure and controlled area, which shall be a designated office, room, or area. The following security precautions will apply to the controlled area:

1. Limited unauthorized personnel access to the area during times that criminal justice information is being processed or viewed.

2. The controlled area shall be locked at all times when not in use or attended by an authorized individual.

3. Information systems devices (e.g., computer screens) and physical documents, when in use, shall be positioned to prevent unauthorized individuals from being able to access or view them.

4. Encryption shall be used for digital storage of criminal justice information. (See AG 8321)

H. Passwords (Standard Authentication)[2]

All authorized individuals with access to computer or systems where processing is conducted or containing criminal justice information must have a unique password to gain access. This password shall not be used for any other account to which the individual has access and shall comply with the following attributes and standards.

1. at least eight (8) characters long on all systems

2. not be a proper name or a word found in the dictionary

3. not be the same as the user identification

4. not be displayed when entered into the system (must use feature to hide password as typed)

5. not be transmitted in the clear outside of the secure location used for criminal justice information storage and retrieval

6. must expire and be changed every ninety (90) days

7. renewed password cannot be the same as any prior ten (10) passwords used (See also, AG 8321)

[2]Applicable to districts that maintain CHRI within a digital system of records, such as a digital database, filing system, record keeping software, spreadsheets, etc. Not applicable if CHRI kept solely via e-mail and/or paper copies.

I. Security Awareness Training

All individuals who are authorized by the District to have access to criminal justice information or to systems which store criminal justice information shall have basic security awareness training within six (6) months of initial assignment/authorization and every two (2) years thereafter. The training shall, to the extent possible, be received through a program approved by the Michigan State Police. A template of the training is provided on the Michigan State Police's website. At a minimum, the training shall comply with the standards established by the U.S. Department of Justice and Federal Bureau of Investigation for Criminal Justice Information Services. (See AG 8321.) A record shall be kept current of all individuals who have completed the security awareness training.

J. Secondary Dissemination of Information

If criminal history background information received from the Michigan State Police is released to another authorized agency under the sharing provision designated by The Revised School Code, a log of such releases shall be maintained and kept current indicating:

1. the date of release;

2. record disseminated;

3. method of sharing;

4. agency personnel that shared the CHRI;

5. the agency, and name of the individual at the agency, to which the information was released;

6. whether an authorization was obtained.

A log entry need not be kept if the receiving agency/entity is part of the primary information exchange agreements between the District and the Michigan State Police. A release form consenting to the sharing of CHRI shall be maintained at all relevant times.

If CHRI is received from another District or outside agency, an Internet Criminal History Access Tool (ICHAT) background check shall be performed to ensure the CHRI is based on personal identifying information, including the individual's name, sex, and date of birth, at a minimum.

K. Auditing and Accountability

The District's information system shall generate audit records for the events listed below. The District shall specify which information system components shall carry out auditing activities.

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 event 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 account 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 event occurred; 3) type of event; 4) user identity; and 5) outcome (success or failure) of the event.

The District's information system shall provide alerts to the appropriate District officials in the event of an audit processing failure. Audit processing failures include, for example software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

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 one (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.

Ref: Criminal Justice Information Services - Security Policy (Version 5.6, 2017), U.S. Dept. of Justice and Federal Bureau of Investigation
Noncriminal Justice Agency Compliance Audit Review, Michigan State Police, Criminal Justice Information Center, Audit and Training Section
Conducting Criminal Background Checks, Michigan State Police, Criminal Justice Information Center

NEW POLICY - VOL. 32, NO. 1

ADMINISTRATOR DISCIPLINE

Whenever it becomes necessary to discipline an Administrator, the Superintendent shall utilize the following principles and procedures. The Board, or its designee, shall utilize the following principles and procedures if the Superintendent is the subject of the disciplinary action.

The Superintendent/Board shall conduct an investigation of any alleged act or omission by an Administrator that could result in disciplinary action. The Administrator shall be provided with oral or written notice of the issue or incident being investigated.

The investigation shall include, at a minimum, interviews of appropriate persons and a meeting with the subject Administrator to allow the Administrator an opportunity to respond to the complaint. Prior notice of this meeting shall be provided to the Administrator for any discipline that may result in a suspension or loss of pay.

After completion of the investigation, if discipline is to be imposed, the Administrator shall receive written notice of the discipline and this notice shall also be placed in the Administrator's file.

Discipline may include, but is not limited to:

A. written warning;

B. written reprimand;

C. suspension (paid or unpaid);

D. discharge;

E. financial penalty in accordance with Michigan law.

The District does not have to apply discipline in a progressive manner, but, rather, may impose discipline consistent with seriousness of the Administrator's conduct, as determined by the District. Additionally, nothing in this policy limits the District's right to take other appropriate action, such as placing an Administrator on administrative leave during the pendency of an investigation or issuing a counseling memorandum, which is considered instructional, not disciplinary.

[ ] If it appears that disciplinary action beyond written reprimand may be necessary, the Superintendent should contact the Board to discuss the disciplinary action that is to be taken.

[X] The Superintendent's decision to impose any disciplinary action that is not subject to Board review is final.

Discharge, demotion or non-renewal of an Administrator may only be imposed by the Board in adherence with the requirements of the Revised School Code.

REVISED POLICY - VOL. 32, NO. 1

STAFF DISCIPLINE

Whenever it becomes necessary to discipline a member of the staff, the Superintendent shall utilize related procedures described in the current negotiated agreement, to the extent not inconsistent with the current negotiated agreement, the following principles and procedures.
A teacher may only be discharged, demoted or otherwise disciplined for a reason that is not arbitrary or capricious. In all instances, discipline, discharge and demotion shall occur in accordance with the statutory requirements under the Teacher Tenure Act and the Revised School Code.

The administrator/Superintendent shall conduct an investigation of any alleged act or omission by a teacher that could result in disciplinary action. The teacher shall be provided with oral or written notice of the issue or incident being investigated.

The investigation shall include, at a minimum, interviews of appropriate persons and a meeting with the subject teacher and, if requested or if required by the bargaining agreement, his/her designated representative (either another employee or a union representative if part of a bargaining unit) to allow the teacher an opportunity to respond to the complaint. Prior notice of this meeting shall be provided to the teacher for any discipline that may result in a suspension or loss of pay. The meeting shall not proceed without the teacher's designated representative; however, the meeting shall not be unduly delayed to secure the attendance of the teacher's preferred representative. The District may substitute another representative from the union to timely process the investigation.

After completion of the investigation, if discipline is to be imposed, the teacher shall receive written notice of the discipline and this notice shall also be placed in the teacher's file.

Discipline may include, but is not limited to:

A. written warning;

B. written reprimand;

C. suspension (paid or unpaid);

D. discharge

E. financial penalty in accordance with Michigan law.

The District does not have to apply discipline in a progressive manner, but, rather, may impose discipline consistent with the seriousness of the teacher's conduct, as determined by the District. Additionally, nothing in this policy limits the District's right to take other appropriate action, such as placing a teacher on administrative leave during the pendency of an investigation or issuing a counseling memorandum, which is considered instructional, not disciplinary.

[X] If it appears that disciplinary action beyond written reprimand may be necessary, the administrator should contact the Superintendent to discuss the disciplinary action that is to be taken.

[X] **[only applicable if original investigation conducted by another administrator]** Any disciplinary action that is not subject to Board review as described below may be submitted to the Superintendent for review within five (5) work days of the teacher's receipt of the written confirmation. The Superintendent is not required to conduct an independent investigation. S/He shall meet with the administrator who issued the discipline and with the teacher and his/her designated representative, if requested. The Superintendent may affirm, revise or reject any disciplinary action taken against a teacher and his/her decision is final.

[ ] The administrator's decision to impose any disciplinary action that is not subject to Board review, as described below, is final.

The following disciplinary actions may only be imposed by the Board in adherence with the requirements of the Teacher Tenure Act:

A. discharge of a tenured or probationary teacher;

B. demotion of a tenured teacher (which includes suspension for fifteen (15) or more consecutive days without pay or a reduction in compensation by more than equivalent of thirty (30) days compensation in one (1) school year);

C. non-renewal of a probationary teacher;

M.C.L. 38.101 et seq., 38.74, 380.1230d, 380.1535a

REVISED POLICY - VOL. 32, NO. 1

STAFF DISCIPLINE

Whenever it becomes necessary to discipline a member of the staff, the Board of Education directs the Superintendent to utilize the procedures set out below and any related procedures described in the current negotiated agreement, if applicable.

The Superintendent or his/her designee shall conduct an investigation of any alleged act or omission that could lead to disciplinary action, as appropriate to the situation. The investigation shall include, at a minimum, providing the employee with reasonable notice and the opportunity to respond to the complaint. If the investigation includes a meeting with the employee, prior notice of this meeting shall be provided to the employee for any discipline that may result in a suspension or loss of pay. The meeting shall not proceed without the employee's designated representative; however, the meeting shall not be unduly delayed to secure the attendance of the preferred representative. The District may substitute another representative from the union to timely process the investigation.

Discipline may include, but is not limited to:

A. written warning;

B. written reprimand;

C. suspension (paid or unpaid);

D. discharge;

E. financial penalty in accordance with Michigan law.

The District does not have to apply discipline in a progressive manner, but, rather, may impose discipline consistent with the seriousness of the staff member's conduct, as determined by the District.

The Board

(X) strongly recommends

( ) requires

that before a suspension or termination is invoked the Superintendent contact the school attorney.

The Board requires that all disciplinary actions involving loss of pay, suspension or termination be submitted to the Board for review

( ) prior to the action being taken.

(X) as soon as possible after the action has been taken.

The Superintendent should ascertain whether or not the staff member wishes such a report to be made in a closed session of the Board, if a closed session is permitted by the Open Meetings Act.

NEW POLICY - VOL. 32, NO. 1

PROHIBITION OF REFERRAL OR ASSISTANCE

In accordance with Michigan statute, any officer, agent, or employee of the Board of Education is prohibited from referring a student for an abortion or assisting a student in obtaining an abortion.

Whenever it becomes necessary to discipline a member of the staff for violation of this policy, the Superintendent shall utilize related procedures described in the Staff Discipline Policy 1439, Policy 3139, and Policy 4139 or the current negotiated agreement, if applicable.

Using due-process procedures, the Superintendent shall conduct an investigation, as appropriate to the situation, including providing the employee with reasonable notice and the opportunity to respond.

If it is determined that any officer, agent, or employee of the Board has violated this policy, the Board shall apply a financial penalty against such individual that is equivalent to not less than three percent (3%) of that individual's annual compensation.

The District shall refund to the State School Aid fund an amount of money equal to the amount of the penalty or fine.

M.C.L. 388.1766

REVISED POLICY - VOL. 32, NO. 1

REPRODUCTIVE HEALTH AND FAMILY PLANNING

The Board of Education directs that instruction be provided on the principal modes by which dangerous communicable diseases, including HIV and AIDS, are spread and the best methods for the restriction and prevention of these diseases. The instruction shall stress that abstinence from sex is the only protection that is 100% effective against unplanned pregnancy and sexually transmitted diseases, including HIV and AIDS, and that abstinence is a positive lifestyle for unmarried young people. No person shall dispense or otherwise distribute in a District school or on District school property a family planning drug or device. Additionally, any officer, agent, or employee of the Board is prohibited from referring a student for an abortion or assisting a student in obtaining an abortion.

The Board accepts as policy the guidelines entitled "Sex Education Guidelines including Reproductive Health and Family Planning" established by the Michigan Department of Education. A copy shall be available for inspection in the Board office.

Each person who teaches K to 12 students about human immunodeficiency virus infection and acquired immunodeficiency syndrome shall have training in human immunodeficiency virus infection and acquired immunodeficiency syndrome education for young people. Licensed health care professionals who have received training on human immunodeficiency virus infection and acquired immunodeficiency syndrome are exempt from this requirement.

The District shall notify the parents, in advance of the instruction and about the content of the instruction, give the parents an opportunity, prior to instruction, to review the materials to be used (other than tests), as well as the opportunity to observe the instruction, and advise the parents of their right to have their child excused from the instruction.

Before any revisions to the curriculum on the subjects taught pursuant to M.C.L. 380.1169 are implemented, the Board shall hold at least two (2) public hearings on the proposed revisions. The hearings shall be held at least one (1) week apart and public notice of the hearings shall be given in the manner required for board meetings. A public hearing held pursuant to this section may be held in conjunction with a public hearing held pursuant to M.C.L. 380.1507.

M.C.L. 380.1169, 380.1507, 388.1766
A.C. Rule 388.273 et seq.

REPLACEMENT POLICY – SPECIAL UPDATE MAY 2017

STUDENT SECLUSION AND RESTRAINT

This policy is intended to provide the framework for organizational supports that result in effective interventions based on team-based leadership, data-based decision-making, continuous monitoring of student behavior, regular universal screening and effective on-going professional development. The District is committed to investing in prevention efforts and to teach, practice and reinforce behaviors that result in positive academic and social outcomes for students.

In the event that staff members need to restrain and/or seclude students, it must be done in accordance with this policy, which is intended to:

A. promote the care, safety, welfare and security of the school community and the dignity of each student;

B. encourage the use of proactive, effective, evidence and research based strategies and best practices to reduce the occurrence of challenging behaviors, eliminate the use of seclusion and restraint, and increase meaningful instructional time for all students; and

C. ensure that seclusion and restraint are used only as a last resort in an emergency situation and are subject to diligent assessment, monitoring, documentation and reporting by trained personnel.

In furtherance of these objectives, the District will utilize Positive Behavioral Interventions and Supports (PBIS) to enhance academic and social behavior outcomes for all students. PBIS implemented by the District will include socially valued and measurable outcomes, empirically validated and practical practices, systems that efficiently and effectively support implementation of these practices, and continuous collection and use of data for decision-making.

EMERGENCY SECLUSION

A. **Prohibited Practices and Limitations on Use**

The following practices are prohibited under all circumstances, including emergency situations:

1. confinement of students who are severely self-injurious or suicidal

2. corporal punishment, as defined in M.C.L. 380.1312(1) of the revised school code, 1976 PA 451

3. the deprivation of basic needs

4. anything constituting child abuse

5. seclusion of pre-school children

6. seclusion that is used for the convenience of school personnel

7. seclusion as a substitute for an educational program

8. seclusion as a form of discipline or punishment

9. seclusion as a substitute for less restrictive alternatives, adequate staffing or school personnel training in PBIS

10. when contraindicated based on (as documented in a record or records made available to the school) a student's disability, health care needs, or medical or psychiatric condition

B. **Definition of Emergency Seclusion**

Seclusion means the confinement of a student in a room or other space from which the student is physically prevented from leaving. Seclusion does not include the general confinement of students if that confinement is an integral part of an emergency lockdown drill required under Section 19(5) of the Fire Prevention Code, 1941 PA 207, M.C.L. 29.19, or of another emergency security procedure that is necessary to protect the safety of students.

Emergency seclusion is a last resort emergency safety intervention involving seclusion that is necessitated by an ongoing emergency situation and that provides an opportunity for the student to regain self-control while maintaining the safety of the student and others.

To qualify as emergency seclusion, there must be continuous observation by school personnel of the student and the room or area used for confinement:

1. must not be locked

2. must not prevent the student from exiting the area should staff become incapacitated or leave that area

3. must provide for adequate space, lighting, ventilation, viewing, and the safety of the student

4. must comply with State and local fire and building codes

C. **Time and Duration** Emergency seclusion should not be used any longer than necessary, based on research and evidence, to allow a student to regain control of his/her behavior to the point that the emergency situation necessitating the use of emergency seclusion is ended, but generally no longer than:

1. fifteen (15) minutes for an elementary school student;

2. twenty (20) minutes for a middle school or high school student

If an emergency seclusion lasts longer than the suggested maximum times above, the following are required:

1. additional support (which may include change of staff, introducing a nurse or specialist, or additional key identified personnel)

2. documentation to explain the extension beyond the time limit

Additional procedures and requirements applicable to both seclusion and restraint are set out below.

EMERGENCY RESTRAINT

A. **Prohibited Practices**

The following procedures are prohibited under all circumstances, including emergency situations:

1. mechanical restraint

2. chemical restraint

3. corporal punishment as defined in 380.1312(1) of the revised school code, 1976 PA 451, otherwise known as the Corporal Punishment Act

4. the deprivation of basic needs

5. anything constituting child abuse

6. restraint that is used for the convenience of school personnel

7. restraint as a substitute for an educational program

8. restraint as a form of discipline or punishment

9. restraint as a substitute for less restrictive alternatives, adequate staffing or school personnel training in PBIS

10. when contraindicated based on (as documented in a record or records made available to the school) a student's disability, health care needs, or medical or psychiatric condition

11. any restraint that negatively impacts breathing, including any positions, whether on the floor, facedown, seated or kneeling, in which the student's physical position (e.g., bent over) is such that it is difficult to breathe, including situations that involve sitting or lying across an individual's back or stomach

12. prone restraint (the restraint of a person face down)

    NOTE: School personnel who find themselves involved in the use of a prone restraint as the result of responding to an emergency must take immediate steps to end the prone restraint.

13. the intentional application of any noxious substance(s) or stimuli that results in physical pain or extreme discomfort

    A noxious substance or stimuli can either be generally acknowledged or specific to the student.

14. physical restraint, other than emergency physical restraint

15. any other type of restraint not expressly allowed

B. **Definition of Restraint**

Restraint means an action that prevents or significantly restricts a student's movement. Physical restraint is intended for the purposes of emergency situations only, in which a student's behavior poses imminent risk to the safety of the individual student or to the safety of others. An emergency situation requires an immediate intervention.

Emergency physical restraint is a last resort emergency safety intervention involving physical restraint that is necessitated by an ongoing emergency situation and that provide an opportunity for the student to retain self-control while maintaining the safety of the student and others. An emergency situation requires an immediate intervention. Emergency physical restraint may not be used in place of appropriate less restrictive interventions.

There are three (3) types of restraint: physical, chemical, and mechanical.

1. **Physical restraint** involves direct physical contact.

   Restraint does not include actions undertaken for the following reasons:

   a. to break up a fight

   b. to take a weapon away from a student

   c. to briefly hold the student (by an adult) in order to calm or comfort him/her

   d. to have the minimum contact necessary to physically escort a student from one area to another

   e. to assist a student in completing a task/response if the student does not resist or if resistance is minimal in intensity or duration

   f. to hold a student for a brief time in order to prevent an impulsive behavior that threatens the student's immediate safety (e.g., running in front of a car)

   g. to stop a physical assault as defined in M.C.L. 380.1310

   h. actions that are an integral part of a sporting event, such as a referee pulling football players off from a pile or similar action

2. **Chemical Restraint** is the administration of medication for the purpose of restraint.

   Restraint does not include administration of medication prescribed by and administered in accordance with the directions of a physician.

3. **Mechanical Restraint** means the use of any device, article, garment, or material attached to or adjacent to a student's body to perform restraint.

   Restraint does not include the following:

   a. an adaptive or protective device recommended by a physician or therapist (when it is used as recommended)

   b. safety equipment used by the general student population as intended (e.g., seat belts, safety harness on school transportation)

C. **Time and Duration**

Restraint should not be used:

1. any longer than necessary, based on research and evidence, to allow students to regain control of their behavior to the point that the emergency situation necessitating the use of emergency physical restraint is ended; and

2. generally no longer than ten (10) minutes.

If an emergency restraint lasts longer than ten (10) minutes, all of the following are required:

1. additional support, which may include a change of staff, or introducing a nurse, specialist, or additional key identified personnel

2. documentation to explain the extension beyond the time limit

Additional procedures and requirements applicable to both seclusion and restraint are set out below.

USE OF EMERGENCY SECLUSION/RESTRAINT

A. **When to Use Emergency Seclusion/Restraint**

Seclusion/restraint must be used only under emergency situations and if essential. Emergency situation means a situation in which a student's behavior poses imminent risk to the safety of the individual student or to the safety of others. An emergency situation requires an immediate intervention.

B. **General Procedures for Emergency Seclusion/Restraint:**

1. An emergency seclusion/restraint may not be used in place of appropriate, less restrictive interventions.

2. Emergency seclusion/restraint shall be performed in a manner that is:

   a. safe;

   b. appropriate; and

   c. proportionate to and sensitive to the student's:

      1) severity of behavior;

      2) chronological and developmental age;

      3) physical size;

      4) gender;

      5) physical condition;

      6) medical condition;

7) psychiatric condition; and

8) personal history, including any history of physical or sexual abuse or other trauma.

3. School personnel shall call key identified personnel for help from within the school building either immediately at the onset of an emergency situation or, if it is reasonable under the particular circumstances for school personnel to believe that diverting their attention to calling for help would increase the risk to the safety of the student or to the safety of others, as soon as possible once the circumstances no longer support such a belief.

4. While using emergency seclusion/restraint, staff must do all of the following:

a. involve key identified personnel to protect the care, welfare, dignity, and safety of the student

b. continually observe the student in emergency seclusion for indications of physical distress and seek medical assistance if there is a concern

c. document observations

d. ensure to the extent practicable, in light of the ongoing emergency situation, that the emergency seclusion/restraint does not interfere with the student's ability to communicate using the student's primary mode of communication

e. ensure that at all times during the use of emergency seclusion/restraint there are school personnel present who can communicate with the student using the student's primary mode of communication

5. Each use of an emergency seclusion/restraint and the reason for each use shall be documented and reported according to the following procedures:

    a. document in writing and report in writing or orally to the building administration immediately

    b. report in writing or orally to the parent or guardian immediately

    c. a report shall be written for each use of seclusion/restraint (including multiple uses within a given day) and the written report(s) provided to the parent or guardian within the earlier of one (1) school day or seven (7) calendar days

6. After any use of an emergency seclusion/restraint, staff must make reasonable efforts to debrief and consult with the parent or guardian, or the parent or guardian and the student (as appropriate) regarding the determination of future actions.

C. **Students Exhibiting a Pattern of Behavior**

If a student exhibits a pattern of behavior that poses a substantial risk of creating an emergency situation in the future that could result in the use of emergency seclusion/restraint, school personnel should do the following:

1. conduct a functional behavioral assessment

2. develop or revise a PBIS plan to facilitate the reduction or elimination of the use of seclusion/restraint

3. develop an assessment and planning process conducted by a team knowledgeable about the student, including at least:

    a. the parent or guardian

    b. the student (if appropriate)

    c. people who are responsible for implementation of the PBIS plan

    d. people who are knowledgeable in PBIS

4. develop a written emergency intervention plan ("EIP") to protect the health, safety, and dignity of the student. An EIP may not expand the legally permissible use of emergency seclusion/restraint.

The EIP should be developed by a team in partnership with the parent or guardian. The team shall include:

1. a teacher;

2. an individual knowledgeable about legally permissibly use of seclusion/restraint; and

3. an individual knowledgeable about the use of PBIS to eliminate the use of seclusion/restraint.

The EIP should be developed and implemented by taking all of the following documented steps:

1. describe in detail the emergency intervention procedures

2. describe in detail the legal limits on the use of emergency seclusion/restraint, including examples of legally permissible and prohibited uses

3. inquire of the student's medical personnel (with parent or guardian consent) regarding any known medical or health contraindications for the use of seclusion/restraint

4. conduct a peer review by knowledgeable staff

5. provide the parent or guardian with all of the following, in writing and orally:

    a. A detailed explanation of the PBIS strategies that will reduce the risk of the student's behavior creating an emergency situation.

    b. An explanation of what constitutes an emergency, including examples of situations that would fall within and outside of the definition.

    c. A detailed explanation of the intervention procedures to be followed in an emergency situation, including the potential use of emergency seclusion/restraint.

    d. A description of possible discomforts or risks.

    e. A detailed explanation of the legal limits on the use of emergency seclusion/restraint, including examples of legally permissible and prohibited uses.

    f. Answers to any questions.

A student who is the subject of an EIP should be told or shown the circumstances under which emergency intervention could be used.

D. **Data Collection and Reporting**

The building administrator shall develop a system of data collection, collect the data and forward all incident reports and data regarding the use of seclusion/restraint to the **Superintendent**.

The data must:

1. be analyzed to determine the efficacy of the school's school-wide system of behavioral support;

2. be analyzed in the context of suspension, expulsion, and dropout data;

3. be analyzed for the purposes of continuous improvement of training and technical assistance toward the reduction or elimination of seclusion/restraint;

4. be analyzed on a schedule determined by the Michigan Department of Education (MDE);`

5. be reported to the MDE, if and as required;

6. include a list of appropriately trained, identified personnel and their levels of:

    a. education;

    b. training; and

    c. knowledge.

NOTE: The District must report to the MDE on the use of seclusion and restraint periodically. MDE will develop guidelines that outline the process for reporting redacted, aggregated data regarding the emergency use of seclusion and restraint.

Training Framework

A comprehensive training framework will be implemented which includes the following:

A. awareness training for all school personnel who have regular contact with students; and

B. comprehensive training for key identified personnel.

All substitute teachers must be informed of and understand the procedures regarding the use of emergency seclusion and emergency restraint. This requirement may be satisfied using online training developed or approved by MDE and online acknowledgement of understanding and completion of the training by the substitute teacher.

Comprehensive Training for Identified Personnel

Each building administrator will identify sufficient key personnel to ensure that trained personnel are generally available for an emergency situation. Before using emergency seclusion or emergency physical restraint with students, key identified personnel who may have to respond to an emergency safety situation must be trained in all of the following:

A. proactive practices and strategies that ensure the dignity of students

B. conflict resolution

C. mediation

D. social skills training

E. de-escalation techniques

F. positive behavioral intervention and support strategies

G. techniques to identify student behaviors that may trigger emergency safety situations

H. related safety considerations, including information regarding the increased risk of injury to students and staff when seclusion or restraint is used

I. instruction in the use of emergency seclusion and emergency physical restraint

J. identification of events and environmental factors that may trigger emergency safety situations

K. instruction on the State policy on the use of seclusion and restraint

L. description and identification of dangerous behaviors

M. methods for evaluating the risk of harm to determine whether the use of emergency seclusion or emergency physical restraint is warranted

N. types of seclusion

O. types of restraint

P. the risk of using seclusion and restraint in consideration of a student's known and unknown medical or psychological limitations

Q. cardiopulmonary resuscitation and first aid

R. the effects of seclusion and restraint on all students

S. how to monitor for and identify physical signs of distress and the implications for students generally and for students with particular physical or mental health conditions or psychological limitations

T. ways to obtain appropriate medical assistance

GLOSSARY OF TERMS

"**Chemical Restraint**" means the administration of medication for the purpose of restraint.

"**De-escalation Techniques**" means evidence- and research-based strategically employed verbal or nonverbal interventions used to reduce the intensity of threatening behavior before, during, and after a crisis situation occurs.

"**Documentation**" means documentation developed by the Michigan Department of Education that is uniform across the State.

"**Emergency Situation**" means a situation in which a student's behavior poses imminent risk to the safety of the individual student or to the safety of others. An emergency situation requires an immediate intervention.

"**Functional Behavioral Assessment**" means an evidence- and research-based systematic process for identifying the events that trigger and maintain problem behavior in an educational setting. A functional behavioral assessment shall describe specific problematic behaviors, report the frequency of the behaviors, assess environmental and other setting conditions where problematic behaviors occur, and identify the factors that are maintaining the behaviors over time.

"**Key Identified Personnel**" means those individuals who have received the mandatory training described in M.C.L. 380.1307G(B)(I) to (XVI), listed under Comprehensive Training for Identified Personnel above.

"**Mechanical Restraint**" means the use of any device, article, garment, or material attached to or adjacent to a student's body to perform restraint.

"**Physical Restraint**" means restraint involving direct physical contact.

"**Positive Behavioral Intervention and Support (PBIS)**" means a framework to assist school personnel in adopting and organizing evidence-based behavioral interventions into an integrated continuum of intensifying supports based on student need that unites examination of the function of the problem behavior and the teaching of alternative skill repertoires to enhance academic and social behavior outcomes for all students.

"**Positive Behavioral Intervention and Support Plan**" means a student-specific support plan composed of individualized, functional behavioral assessment-based intervention strategies, including, as appropriate to the student, guidance or instruction for the student to use new skills as a replacement for problem behaviors, some rearrangement of the antecedent environment so that problems can be prevented and desirable behaviors can be encouraged, and procedures for monitoring, evaluating, and modifying the plan as necessary.

"**Prone Restraint**" means the restraint of an individual face down.

"**Regularly and Continuously Work Under Contract**" means that term as defined in section M.C.L. 380.1230.

"**Restraint**" means an action that prevents or significantly restricts a student's movement. Restraint does not include the brief holding of a student in order to calm or comfort, the minimum contact necessary to physically escort a student from one area to another, the minimum contact necessary to assist a student in completing a task or response if the student does not resist or resistance is minimal in intensity or duration, or the holding of a student for a brief time in order to prevent an impulsive behavior that threatens the student's immediate safety, such as running in front of a car. Restraint does not include the administration of medication prescribed by and administered in accordance with the directions of a physician, an adaptive or protective device recommended by a physician or therapist when it is used as recommended, or safety equipment used by the general student population as intended, such as a seat belt or safety harness on school transportation. Restraint does not include necessary actions taken to break up a fight, to stop a physical assault, as defined in M.C.L. 380.1310, or to take a weapon from a student. Restraint does not include actions that are an integral part of a sporting event, such as a referee pulling football players off of a pile or a similar action.

Restraint that negatively impacts breathing means any restraint that inhibits breathing, including floor restraints, facedown position, or any position in which an individual is bent over in such a way that it is difficult to breathe. This includes a seated or kneeling position in which an individual being restrained is bent over at the waist and restraint that involves sitting or lying across an individual's back or stomach.

"**School Personnel**" includes all individuals employed in a public school or assigned to regularly and continuously work under contract or under agreement in a public school, or public school personnel providing service at a nonpublic school.

"**Seclusion**" means the confinement of a student in a room or other space from which the student is physically prevented from leaving. Seclusion does not include the general confinement of students if that confinement is an integral part of an emergency lockdown drill required under Section 19(5) of the Fire Prevention Code, 1941 PA 207, M.C.L. 29.19, or of another emergency security procedure that is necessary to protect the safety of student.

Adapted from Michigan State Board of Education Policy for the Emergency Use of Seclusion and Restraint adopted in March of 2017

Information & Technology Collection - supplement

POLICY 7540.03 - STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

The substantive changes in this policy include the following:

1. References to the definitions of Technology Resources and Information Resources in Bylaw 0100 are added in the first paragraph.

2. The terms “Technology Resources” and “Information Resources” are capitalized throughout to indicate that they are terms of art for which there are specific definitions applicable to the District’s policies.

3. Clarify that the Board intends to regulate the use of District Technology Resources in accordance with applicable local, State and Federal laws, the District's educational mission, and the terms of the Student Code of Conduct.

4. State that personal communication devices (PCDs) when connected to the District's Technology Resources are also subject to the terms of this policy.

5. Remind users that they must refrain from engaging in illegal or unkind actions, and provide examples of what is meant by illegal and unkind actions.

6. Added language clarifying when students may use District Technology Resources to access and use social media for educational purposes.

REVISED POLICY - TECHNOLOGY UPDATE – PHASE III

STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board of Education provides Technology Resources (as defined in Bylaw 0100) to support the educational and professional needs of its students and staff. With respect to students, District Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students. The District's computer network and Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District Technology Resources by principles consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. This policy and its related administrative guidelines and the Student Code of Conduct govern students' use of District Technology Resources and students'personal communication devices when they are connected to the District computer network, Internet connection, and/or online educational services/apps, or when used while the student is on Board-owned property or at a Board-sponsored activity (see Policy 5136).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

First, the Board may not be able to technologically limit access, through its Technology Resources, to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using District Technology Resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or Technology Director may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

Parents are advised that a determined user may be able to gain access to services and/or resources on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents may find inappropriate, offensive, objectionable or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.
Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications

B. the dangers inherent with the online disclosure of personally identifiable information

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students online, and

D. unauthorized disclosure, use, and dissemination of personally-identifiable information regarding minors

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while at school.

[x] Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of District Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including in chat rooms, and cyberbullying awareness and response. All users of District Technology Resources (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

[x] Students will be assigned a school e-mail account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. (x) Further, as directed and authorized by their teachers, they shall use their school-assigned e-mail account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

Students are responsible for good behavior when using District Technology Resources – i.e., behavior comparable to that expected of students when they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not approve any use of its Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

[NOTE: If language about social media is added to Policy 7540, it is recommended that this language be added to this policy.]

[ ] Students may only use District Technology Resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Technology Director as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Technology Resources.

P.L. 106-554, Children's Internet Protection Act of 2000
P.L. 110-385, Title II, Protecting Children in the 21st Century Act
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6777, 9134 (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
47 C.F.R. 54.500 – 54.523

Information & Technology Collection - supplement

POLICY 7540.04 – STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

The substantive changes in this policy include the following:

1. References to the definitions of Technology Resources and Information Resources in Bylaw 0100 are added in the first paragraph.

2. The terms “Technology Resources” and “Information Resources” are capitalized throughout to indicate they are terms of art for which there are specific definitions applicable to the District's policies.

3. Clarify that the Board intends to regulate the use of District Technology and Information Resources in a manner consistent with applicable local, State, and Federal laws, as well as the District's educational mission.

4. State that use of Technology Resources and Information Resources, along with personal communication devices (PCDs), are subject to the Board’s acceptable use policy.

5. On page 2, we include a more general overview statement that requires users to refrain from engaging in illegal and unkind actions, and we include examples of what is meant by illegal and unkind actions.

6. We deleted the reference to users’ due process rights because they are not unique to this area – i.e., the District is obligated to meet certain due process standards whenever it takes disciplinary actions – and therefore do not need to repeat it here.

7. Inserted a statement that users have no expectations of privacy with regard to their use of both District Technology and Information Resources.

8. Changed the reference to training involving “social networking websites” to training involving “social media” since users often access social networking services through apps instead of websites today.

9. We added new language concerning staff members' use of District Technology Resources to access and use social media for business-related purposes.

REVISED POLICY - TECHNOLOGY UPDATE – PHASE III

STAFF TECHNOLOGY
ACCEPTABLE USE AND SAFETY

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board of Education provides Technology and Information Resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's computer network and Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District Technology and Information Resources by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staffs' use of the District's Technology and Information Resources and staff's personal communication devices when they are connected to the District's computer network, Internet connection and/or online educational services/apps, or when used while the staff member is on Board-owned property or at a Board-sponsored activity (see Policy 7530.02).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology and Information Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff are expected to utilize District Technology and Information Resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services will be guided by Board Policy 2521 – Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that brings incredible education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District Technology Resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

First, the Board may not be able to technologically limit access, through its Technology Resources, to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the District Technology Resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The Superintendent or Technology Director may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. **(X)** The Superintendent or Technology Director may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personally-identifiable information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above, and staff members will monitor students' online activities while at school.

[X] Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the District Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media including in chat rooms, and cyberbullying awareness and response. All users of District Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

[X] Staff will be assigned a school e-mail address that they are required to utilize for all school-related electronic communications, including those to students, parents and other staff members.

[X] With prior approval from the Superintendent or Technology Director, staff may direct students who have been issued school-assigned e-mail accounts to use those accounts when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District Technology and Information Resources - i.e., behavior comparable to that expected when they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its Technology and Information Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

[NOTE: If language about social media is added to Policy 7540, choose the appropriate option to match that language]

[ ] Staff members may only use District Technology Resources to access or use social media if it is done for educational or business-related purposes.

General school rules for behavior and communication apply.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Technology and Information Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Technology Director as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District Technology and Information Resources.

[OPTIONAL]

[x] Social Media Use

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential employee information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

P.L. 106-554, Children's Internet Protection Act of 2000
P.L. 110-385, Title II, Protecting Children in the 21st Century Act
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
47 C.F.R. 54.500 – 54.523

REVISED POLICY - TECHNOLOGY UPDATE – PHASE III

DISTRICT-ISSUED STAFF E-MAIL ACCOUNT

Staff

The Board of Education is committed to the effective use of electronic mail ("e-mail") by all District staff and Board members in the conduct of their official duties. This policy and any corresponding guidelines are intended to establish a framework for the proper use of e-mail for conducting official business and communicating with colleagues, students, parents and community members.

When available, the District's e-mail system must be used by employees for any official District e-mail communications. **(X)** Personal e-mail accounts on providers other than the District's e-mail system

(X) may be blocked at any time

( ) shall be blocked

if concerns for network security, SPAM, or virus protection arise. Furthermore, District staff are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the District's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

District staff shall not send or forward mass e-mails, even if the e-mails concern District business, without prior approval of the

(X) Technology Director or building principal.

( ) site administrator.

( ) _____ **[other]**.

District staff may join list servs or other e-mail services (e.g. RSS feeds) that pertain to their responsibilities in the District, **(X)** provided these list servs or other e-mail services do not exceed the staff member's e-mail storage allotment. **(X)** If a staff member is unsure whether s/he has adequate storage or should subscribe to a list serv or RSS feed, s/he should discuss the issue with his/her building principal or the District's **(X)** Technology Director **or** IT staff. The

(X) Technology Director

( ) site administrator

( ) _____ (other)

is authorized to block e-mail from list servs or e-mail services if the e-mails received by the staff member(s) (X) become excessive ( ) regularly exceed _____ megabytes.

Staff members are encouraged to keep their inbox and folders organized by regularly reviewing e-mail messages, appropriately saving e-mails that constitute a public record or student record and e-mails that are subject to a litigation hold (see Policy 8315 – Information Management), and purging all other e-mails that have been read. If the staff member is concerned that his/her e-mail storage allotment is not sufficient, s/he should contact the District's **(X)** Technology Director **( )** IT staff.

Public Records

The District complies with all Federal and State laws pertaining to electronic mail. Accordingly, e-mails written by or sent to District staff and Board members may be public records if their content concerns District business, or education records if their content includes personally identifiable information about a student. E-mails that are public records are subject to retention and disclosure, upon request, in accordance with Policy 8310 – Public Records. E-mails that are student records must be maintained pursuant to Policy 8330 – Student Records. Finally e-mails may constitute electronically stored information ("ESI") that may be subject to a litigation hold pursuant to Policy 8315 – Information Management.

State and Federal law exempt certain documents and information within documents from disclosure, no matter what their form. Therefore, certain e-mails may be exempt from disclosure or it may be necessary to redact certain content in the e-mails before the e–mails are released pursuant to a public records request, the request of a parent or eligible student to review education records, or a duly served discovery request involving ESI.

E-mails written by or sent to District staff and Board members by means of their private e-mail account may be public records if the content of the e-mails concerns District business, or education records if their content includes personally-identifiable information about a student. Consequently, staff shall comply with a District request to produce copies of e-mail in their possession that are either public records or education records, or that constitute ESI that is subject to alitigation hold, even if such records reside on a computer owned by an individual staff member, or are accessed through an e-mail account not controlled by the District.

Retention

Pursuant to State and Federal law, e-mails that are public records or education records, and e-mails that are subject to a litigation hold shall be retained.

[X] E-mail retention is the responsibility of the individual e-mail user. Users must comply with District guidelines for properly saving/archiving e-mails that are public records, student education records, and/or subject to a litigation hold. The District maintains archives of all e-mails sent and/or received by users of the District's e-mail service for disaster recovery. Staff members are required to forward copies of any work-related e-mails received in their personal e-mail account(s) not affiliated with the District server to their District e-mail account so that these records are also archived for future retrieval, if necessary.Any questions concerning e-mail retention should be directed to the **(X)** Technology Director **( )** site administrator **( )** _____ **[other]**.

[ ]

Unauthorized E-mail

The Board does not authorize the use of its Technology Resources, including its computer network ("network"), to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e-mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send e-mail to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.

Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.

Authorized Use and Training

Pursuant to Policy 7540.04, staff and Board members using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety by signing and submitting Form 7540.04 F1 **(X)** annually.

Furthermore, staff using the District's e-mail system shall satisfactorily complete training **( )**, pursuant to Policy 7540.04, regarding the proper use and retention of e-mail **( )** annually.

NEW POLICY - TECHNOLOGY UPDATE – PHASE III

DISTRICT-ISSUED STUDENT E-MAIL ACCOUNT

Students assigned a school e-mail account are required to utilize it for all school-related electronic communications, including those to staff members and individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned e-mail account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

This policy and any corresponding guidelines serve to establish a framework for student's proper use of e-mail as an educational tool.

Personal e-mail accounts on providers other than the District's e-mail system

(X) may be blocked at any time

if concerns for network security, SPAM, or virus protection arise. Students are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the District's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

Students shall not send or forward mass e-mails, even if educationally-related, without prior approval of their classroom teacher or the

(X) Building Principal.

Students may join list servs or other e-mail services (e.g. RSS feeds) that pertain to academic work, provided the e-mails received from the list servs or other e-mail services do not become excessive. If a student is unsure whether s/he has adequate storage or should subscribe to a list serv or RSS feed, s/he should discuss the issue with his/her classroom teacher, the building principal or the District's Technology or IT staff. The

(X) Technology Director

is authorized to block e-mail from list servs or e-mail services if the e-mails received by the student **(X)** become excessive.

Students are encouraged to keep their inbox and folders organized by regularly reviewing e-mail messages and purging e-mails once they are read and no longer needed for school.

Unauthorized E-mail

The Board does not authorize the use of its Technology Resources, including its computer network ("network"), to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e–mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send e-mail to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.

Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.

Authorized Use and Training

Pursuant to Policy 7540.03, students using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety by acknowledging receipt of guidelines regarding proper use of email as part of the required annual student-parent handbook review.

REVISED POLICY - VOL. 32, NO. 1

CRIMINAL HISTORY RECORD CHECK

Before the District hires any employee (full or part-time) or allows any individual under contract to continuously and regularly work in the schools, a criminal history records check shall be conducted in accordance with State law.

"Under contract" shall apply to individuals, as well as owners and employees of entities, who contract directly with the District or with a third-party vendor, management company, or similar contracting entity, to provide food, custodial, transportation, counseling or administrative services on more than an intermittent or sporadic basis. It shall also apply to individuals or entities providing instructional services to students or related auxiliary services to special education students.

Prior to allowing an individual, who is subject to the criminal history record check requirement, to work in the District, the District shall submit a fingerprint-based check on the individual, using Michigan State Police (MSP) Form RI-030 (7/2012), regardless of whether the individual will work directly for the District or be contracted through a third-party vendor, management company or similar contracting entity ("Private Contractors"). Except as provided below, the report from the MSP must be received, reviewed and approved by the District prior to the individual commencing work.

Such Private Contractors cannot receive or retain criminal history record information ("CHRI").[1] Where the District will contract with a Private Contractor for the services of an individual, the District shall notify the Private Contractor(s), after review of the MSP report, whether the individual has been approved to work within the District. The District may not give any details, including the fact that a criminal history check was run. Notice for approval to work in the District should use the Affidavit of Assignment or similar "red light/green light" procedure.

---

[1] Individuals who act on behalf of the District, work on a regular or continuous basis in the District, are involved in the hiring process of District employees, and have successfully undergone a fingerprint-based criminal history record check by the District, may continue to submit and receive such criminal history record checks on behalf of the District, regardless of their status as employees, contractors, vendors or similar classification.

Should it be necessary to employ a person or contract for a person to maintain continuity of the program prior to receipt of the criminal history report, the Superintendent may contract on a provisional basis until the report is received. Any such provisional hire requires that:

A. the record check has been requested;

B. the applicant has signed a disclosure of all convictions and acknowledges that employment may be terminated if there are discrepancies; and

C. the hiring occurs during the school year or not more than thirty (30) days before the beginning of the school year.

For substitute teachers or substitute bus drivers 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 the individual has no criminal history. Absent such confirmation, a criminal history record check shall be performed.

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.

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 Superintendent 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).

"No separation," for purposes of the preceding paragraph, means a layoff 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.

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 the individual's confidential file, which must be maintained in compliance with Policy 8321 and AG 8321.

When the District receives a report that shows an individual has been convicted of a listed offense under state statutes or any felony, the Superintendent shall take steps to verify that information using public records, in accordance with the procedures provided by the State Department of Education.

Verified convictions may result in termination of employment or rejection of an application. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of a "listed" offense as defined in M.C.L. 28.722. The District will not hire or continue to employ any individual, either directly or as a contracted employee to work regularly and continuously in the schools, who has been convicted of any felony unless both the Superintendent and the Board provide written approval.

The District must report as directed by and to the State Department of Education the verified information regarding conviction for any listed offense or conviction for any felony and the action taken by the District with regard to such conviction. Such report shall be filed within sixty (60) days or receipt of the original report of the conviction.

The Superintendent shall establish the necessary procedures for obtaining from the Criminal Records Division of the State Police any criminal history on the applicant maintained by the State Police. In addition, the Superintendent shall request the State Police to obtain a criminal history records check from the Federal Bureau of Investigation.

An applicant must

(X) submit, at no expense to the District,

or

( ) provide, at the District's expense,

a set of fingerprints, prepared by an entity approved by the Michigan State Police, upon receiving an offer of employment, or as required by State law for continued employment. **In the case of difficult-to-fill positions, the Superintendent may opt to provide fingerprints at the District's expense.**

Confidentiality

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 punishable by a fine up to $10,000.

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 FOIA request.

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

Records may also be released, in accordance with statute, upon the request of a school district, intermediate school district, public school academy or non-public school when the individual is an applicant for employment at such school and there has been no separation from service, as defined in this policy and by statute.

M.C.L. 380.1230 et. seq., 380.1535, 380.1535a, 380.1809, 28.722

REVISED POLICY - VOL. 32, NO. 1

CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY)

The District is required by State law to have the Michigan State Police (MSP) obtain both a State and a Federal Bureau of Investigation (FBI) criminal history record information (CHRI) background check report for all employees of the District and contractors, vendors and their employees who work on a regular and continuous basis in the District. To assure the security, confidentiality, and integrity of the CHRI background check information received from the MSP/FBI, the following standards are established:

A. Sanctions for Non-Compliance

Employees who fail to comply with this policy and any guidelines issued to implement this policy will be subject to discipline for such violations. Discipline will range from counseling and retraining to discharge, based on the nature and severity of the violation. All violations will be recorded in writing, with the corrective action taken. The Superintendent shall review, approve, sign and date all such corrective actions.

B. Local Agency Security Officer (LASO)

The **Executive Director of Human Resources** shall be designated as the District's Security Officer and shall be responsible for overall implementation of this policy and for data and system security. This shall include:

1. ensuring that personnel security screening procedures are being followed as set forth in this policy;

2. ensuring that approved and appropriate security measures are in place and working as expected;

3. supporting policy compliance and instituting the incident response reporting procedures;

4. ensuring that the Michigan State Police are promptly informed of any security incidents involving the abuse or breach of the system and/or access to criminal justice information;

5. to the extent applicable, identifying and documenting how District equipment is connected to the Michigan State Police system;

6. to the extent applicable, identify who is using the Michigan State Police approved hardware, software and firmware, and ensuring that no unauthorized individuals have access to these items.

The District's LASO shall be designated on the appropriate form as prescribed and maintained by the Michigan State Police. A new form shall be submitted every time a new LASO is designated.

C. Agency User Agreements

The District shall enter into any required User Agreement for Release of CHRI ("User Agreement"), and future amendments, by the Michigan State Police necessary to access the required CHRI on applicants, volunteers, and all other statutorily required individuals, such as contractors and vendors and their employees assigned to the District. The LASO shall be responsible for the District's compliance with the terms of any such User Agreement.

D. Personnel Security

All individuals that require access to any criminal justice information shall be subject to the following standards prior to granting of access:

1. Background Checks - A Michigan (or state of residency if other than Michigan) and a national fingerprint-based criminal history record check shall be conducted within thirty (30) days of assignment to a position with direct access to criminal justice information or with direct responsibility to configure and maintain computer systems and networks with direct access to criminal justice information.

    a. A felony conviction of any kind will disqualify an individual for access to criminal justice information.

    b. If any other results/records are returned, the individual shall not be granted access until the LASO reviews and determines access is appropriate. This includes, but is not limited to, any record which indicates the individual may be a fugitive or shows arrests without convictions. Such approval shall be recorded in writing, signed, dated and maintained with the individual's file.

c. If support personnel, contractors or custodial workers need to be in an area where CHRI is maintained or processed, they shall be escorted by or under the supervision of authorized personnel at all times while in those area. Information Technology contractors or vendors will be physically or virtually escorted by authorized personnel anytime said individual have access to facilities, areas, rooms, or an agency's CHRI information system.

2. Subsequent Arrest/Conviction - If an individual granted access to criminal justice information is subsequently arrested and/or convicted, access shall be suspended immediately until the matter is reviewed by the LASO to determine if continued access is appropriate. Such determination shall be recorded in writing, signed, dated and maintained with the individual's file. In the event that the LASO has the arrest/conviction, the Superintendent (if not the designated LASO) shall make the determination. If the Superintendent is also the designated LASO, the determination shall be made by Executive Director of Human Resources. Except that, as noted in D(1)(a), individuals with a felony conviction of any kind will have their access indefinitely suspended.

3. Public Interest Denial - If the LASO determines that access to criminal justice information by any individual would not be in the public interest, access shall be denied whether that person is seeking access or has previously been granted access. Such decision and reasons shall be in writing, signed, dated and maintained in the individual's file.

4. Approval for Access - All requests for access to criminal justice information shall be as specified and approved by the LASO. Any such designee must be a direct employee of the District. The District must maintain a readily accessible list that includes the names of all LASO approved personnel with access to criminal justice information, as well as the reason for providing each individual access. This list shall be made available to Michigan State Police upon request.

5. Termination of Employment/Access – Within twenty-four (24) hours of the termination of employment, all access to criminal justice information shall be terminated immediately for that individual, such as closing the individual's account and/or blocking access to any systems containing such information at the District.

6. Transfer/Re-assignment - When an individual who has been granted access to criminal justice information has been transferred or re-assigned to other duties, the LASO shall determine whether continued access is necessary and appropriate. If not, s/he shall take such steps as necessary to block further access to such information within the twenty-four (24) hour period immediately following the transfer or reassignment.

7. Information Technology Contractors and Vendors[1] – Prior to granting access to criminal justice information to an IT contractor or vendor, identification must be verified via a Michigan (or state of residency if other than Michigan) and national fingerprint-based criminal history record check. A felony conviction of any kind, as well as any outstanding arrest warrant, will disqualify an IT contractor or vendor for access to criminal justice information. A contractor or vendor with a criminal record of any other kind may be granted access if the LASO determines the nature or severity of the misdemeanor offense(s) does not warrant disqualification. If any other results/records are returned, the individual shall not be granted access until the LASO reviews and determines access is appropriate.

E. Media Protection

Access to digital and physical media in all forms, which contains criminal history background information provided by the Michigan State Police through the statutory record check process, is restricted to authorized individuals only. Only individuals involved in the hiring determination of both District employees and volunteers shall be authorized to access digital and physical media containing CHRI.

1. Media Storage and Access – All digital and physical media shall be stored in a physically secure location or 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. Digital media shall be stored on a District or School server. Storage on a third party server, such as cloud service, is not permitted. Storage of digital media must conform to the requirements in AG 8321.

[1]Non-Information Technology contractors or vendors shall not have access to criminal justice information.

2. Media Transport – Digital and physical media shall only be transported upon sufficient justification approved by the LASO. Digital and physical medial shall be protected when being transported outside of a controlled area. Only authorized individuals shall transport the media. Physical media (e.g. printed documents, printed imagery, etc.) shall be transported using a locked container, sealed envelope, or other similarly secure measure. To the extent possible, digital media (e.g., hard drives and removable storage devices such as disks, tapes, flash drives and memory cards) shall be either encrypted and/or be password protected during the transport process. The media shall be directly delivered to the intended person or destination and shall remain in the physical control and custody of the authorized individual at all times during transport. Access shall only be allowed to an authorized individual.

3. Media Disposal/Sanitization – When the CHRI background check is no longer needed, the media upon which it is stored shall either be destroyed or sanitized. The LASO and the Superintendent shall approve in writing the media to be affected. This record shall be maintained by the LASO for a period of at least five (5) years. **[Note: the regulations do not specify a specific period for maintaining this information. This time period is suggested as it will likely cover most statutes of limitation and can be retained in digital format.]**

   a. Digital Media - Sanitization of the media and deletion of the data shall be accomplished by either overwriting at least three (3) times or by degaussing, prior to disposal or reuse of the media. If the media is inoperable or will not be reused, it shall be destroyed by shredding, cutting, or other suitable method to assure that any data will not be retrievable.

   b. Physical Media – Disposal of documents, images or other type of physical record of the criminal history information shall be cross-cut shredded or incinerated. Physical security of the documents and their information shall be maintained during the process by authorized individuals. Documents may not be placed in a waste basket or burn bag for unauthorized individuals to later collect and dispose of.

   All disposal/sanitization shall be either conducted or witnessed by authorized personnel to assure that there is no misappropriation of, or unauthorized access to, the data to be deleted. Written documentation of the steps taken to sanitize or destroy the media shall be maintained for ten (10) years, and must include the date as well as the signatures of the person(s) performing and/or witnessing the process. (See also, AG 8321.)

4. Mobile Devices – A personally owned mobile device (mobile phone, tablet, laptop, etc.) shall not be authorized to access, process, store or transmit criminal justice information unless the District has established and documented the specific terms and conditions for personally owned mobile devices.

F. CHRI Background Check Consent and Documentation

All individuals requested to complete a fingerprint-based CHRI background check must have given written consent-properly signed and dated—at time of application and be notified fingerprints will be used to check the criminal history records of the FBI, prior to completing a fingerprint-based CHRI background check. The most current and unaltered Livescan form (RI-030) will satisfy this requirement and must be retained. Individuals subject to a fingerprint-based CHRI background check shall be provided the opportunity to complete or challenge the accuracy of the individual's criminal history record.

Some type of documentation identifying the position for which a fingerprint-based CHRI background check has been obtained must be retained for every CHRI background check conducted, such as an offer letter, employment agreement, new hire checklist, employment contract, volunteer background check form, etc.

G. Controlled Area/Physical Protection

All CHRI obtained from the Michigan State Police pursuant to the statutorily required background checks shall be maintained in a physically secure and controlled area, which shall be a designated office, room, or area. The following security precautions will apply to the controlled area:

1. Limited unauthorized personnel access to the area during times that criminal justice information is being processed or viewed.

2. The controlled area shall be locked at all times when not in use or attended by an authorized individual.

3. Information systems devices (e.g., computer screens) and physical documents, when in use, shall be positioned to prevent unauthorized individuals from being able to access or view them.

4. Encryption shall be used for digital storage of criminal justice information. (See AG 8321)

H. Passwords (Standard Authentication)[2]

All authorized individuals with access to computer or systems where processing is conducted or containing criminal justice information must have a unique password to gain access. This password shall not be used for any other account to which the individual has access and shall comply with the following attributes and standards.

1. at least eight (8) characters long on all systems

2. not be a proper name or a word found in the dictionary

3. not be the same as the user identification

4. not be displayed when entered into the system (must use feature to hide password as typed)

5. not be transmitted in the clear outside of the secure location used for criminal justice information storage and retrieval

6. must expire and be changed every ninety (90) days

7. renewed password cannot be the same as any prior ten (10) passwords used (See also, AG 8321)

[2]Applicable to districts that maintain CHRI within a digital system of records, such as a digital database, filing system, record keeping software, spreadsheets, etc. Not applicable if CHRI kept solely via e-mail and/or paper copies.

I. Security Awareness Training

All individuals who are authorized by the District to have access to criminal justice information or to systems which store criminal justice information shall have basic security awareness training within six (6) months of initial assignment/authorization and every two (2) years thereafter. The training shall, to the extent possible, be received through a program approved by the Michigan State Police. A template of the training is provided on the Michigan State Police's website. At a minimum, the training shall comply with the standards established by the U.S. Department of Justice and Federal Bureau of Investigation for Criminal Justice Information Services. (See AG 8321.) A record shall be kept current of all individuals who have completed the security awareness training.

J. Secondary Dissemination of Information

If criminal history background information received from the Michigan State Police is released to another authorized agency under the sharing provision designated by The Revised School Code, a log of such releases shall be maintained and kept current indicating:

1. the date of release;

2. record disseminated;

3. method of sharing;

4. agency personnel that shared the CHRI;

5. the agency, and name of the individual at the agency, to which the information was released;

6. whether an authorization was obtained.

A log entry need not be kept if the receiving agency/entity is part of the primary information exchange agreements between the District and the Michigan State Police. A release form consenting to the sharing of CHRI shall be maintained at all relevant times.

If CHRI is received from another District or outside agency, an Internet Criminal History Access Tool (ICHAT) background check shall be performed to ensure the CHRI is based on personal identifying information, including the individual's name, sex, and date of birth, at a minimum.

K. Auditing and Accountability

The District's information system shall generate audit records for the events listed below. The District shall specify which information system components shall carry out auditing activities.

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 event 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 account 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 event occurred; 3) type of event; 4) user identity; and 5) outcome (success or failure) of the event.

The District's information system shall provide alerts to the appropriate District officials in the event of an audit processing failure. Audit processing failures include, for example software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

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 one (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.

Ref: Criminal Justice Information Services - Security Policy (Version 5.6, 2017), U.S. Dept. of Justice and Federal Bureau of Investigation
Noncriminal Justice Agency Compliance Audit Review, Michigan State Police, Criminal Justice Information Center, Audit and Training Section
Conducting Criminal Background Checks, Michigan State Police, Criminal Justice Information Center

REVISED POLICY - VOL. 31, NO. 2

WELLNESS

[DRAFTING NOTE: THE FINAL RULE DOES NOT CHANGE THE PROVISIONS ALLOWING "INFREQUENT" SCHOOL SPONSORED FUND RAISERS. THE OPTIONS SELECTED IN PO 9211 AND 5830 ARE, THEREFORE, NOT AFFECTED BY THESE FINAL RULES]

As required by law, the Board of Education establishes the following wellness policy for the Dexter Community School District.

The Board recognizes that good nutrition and regular physical activity affect the health and well-being of the District's students. Furthermore, research concludes that there is a positive correlation between a student's health and well-being and his/her ability to learn. Moreover, schools can play an important role in the developmental process by which students establish their health and nutrition habits by providing nutritious meals and snacks through the schools' meal programs, by supporting the development of good eating habits, and by promoting increased physical activity both in and out of school.

The Board, however, believes this effort to support the students' development of healthy behaviors and habits with regard to eating and exercise cannot be accomplished by the schools alone. It will be necessary for not only the staff, but also parents and the public at large to be involved in a community-wide effort to promote, support, and model such healthy behaviors and habits.
The Board sets the following goals in an effort to enable students to establish good health and nutrition habits:

A. With regard to nutrition education, the District should:

[Select one or more of the following:]

(X) Nutrition education should include enjoyable, developmentally appropriate and culturally relevant participatory activities, such as contests, promotions, taste testing, and others.

(X) Nutrition education posters, such as the Food Pyramid Guide,

will be displayed in the cafeteria.

(X) The school cafeteria may serve as a learning lab by allowing students to apply the knowledge, attitudes, and skills taught in the classroom when making choices at mealtime.

(X) Nutrition education standards and benchmarks promote the benefits of a balanced diet that includes fruits, vegetables, whole grain products, and low-fat and fat-free dairy products.

B. With regard to physical activity, the District will:

1. Physical Education

(X) A sequential, comprehensive physical education program shall be provided for students in K-12 in accordance with the standards and benchmarks established by the State.

(X) The physical education curriculum shall provide sequential instruction related to the knowledge, attitudes, and skills necessary to participate in lifelong, health-enhancing physical activity.

(X) The K-12 program shall include instruction in physical education as well as opportunities to participate in competitive and non-competitive team sports to encourage lifelong physical activity.

(X) Planned instruction in physical education shall require students to be engaged in moderate to vigorous physical activity for at least fifty percent (50%) of scheduled class time.

(X) Properly certificated, highly qualified teachers shall provide all instruction in physical education.

(X) Planned instruction in physical education shall teach cooperation, fair play, and responsible participation.

(X) Planned instruction in physical education shall meet the needs of all students, including those who are not athletically gifted.

2. Physical Activity

(x) Physical activity **should** not be employed as a form of discipline or punishment.

(xi) All after-school programs should provide developmentally appropriate physical activity for the students who participate.

C. With regard to other school-based activities the District shall:

(X) Students, parents, and other community members should have access to, and be encouraged to use, the school's outdoor physical activity facilities outside the normal school day following posted times and usage policies.

(X) Schools in our system utilize electronic identification and payment systems, therefore, eliminating any stigma or identification of students eligible to receive free and/or reduced meals.

D. With regard to nutrition promotion, any foods and beverages marketed or promoted to students on the school campus, during the school day, will meet or exceed the USDA Smart Snacks in School nutrition standards.

Additionally, the District shall:

(X) create an environment that reinforces the development of healthy eating habits, including offering the following healthy foods that comply with the USDA Dietary Guidelines for Americans and the USDA Smart Snacks in School nutrition standards:

(X) a variety of fresh produce to include those prepared without added fats, sugars, refined sugars, and sodium

(X) a variety of vegetables daily to include specific subgroups as defined by dark green, red/orange, legumes, and starchy

(X) fluid milk that is fat-free (unflavored and flavored) and low-fat (unflavored)

(X) meals designed to meet specific calorie ranges for age/grade groups

(x) eliminate trans-fat from school meals

(x) require students to select a fruit or vegetable as part of a complete reimbursable meal

(x) provide opportunities for students to develop the knowledge and skills for consuming healthful foods

(x) The District nutrition department will promote and encourage Farm to School efforts in order to provide the healthy foods identified above.

Furthermore, with the objectives of enhancing student health and well being, and reducing childhood obesity, the following guidelines are established:

A. In accordance with Policy 8500, entitled Food Service, the food service program shall comply with Federal and State regulations pertaining to the selection, preparation, consumption, and disposal of food and beverages, including but not limited to the USDA Dietary Guidelines for Americans and the USDA Smart Snacks in School nutrition standards, as well as to the fiscal management of the program.

B. As set forth in Policy 8531, entitled Free and Reduced Price Meals, the guidelines for reimbursable school meals are not less restrictive than the guidelines issued by the U.S. Department of Agriculture (USDA).

   The sale of foods of minimal nutritional value in the food service area during the lunch period is prohibited.

C. The sale of foods and beverages to students that do not meet the USDA Dietary Guidelines for Americans and the USDA Smart Snacks in School nutrition standards to be consumed on the school campus during the school day is discouraged.

D. All food items and beverages available for sale to students for consumption on the school campus (any area of property under the jurisdiction of the school that is accessible to students during the school day) between midnight and thirty (30) minutes after the close of the regular school day shall comply with the current USDA Dietary Guidelines for Americans and the USDA Smart Snacks in School nutrition standards, including, but not limited to, competitive foods that are available to students a la carte or as entrees in the dining area (except entree items that were offered on the National School Lunch Program (NSLP) or School Breakfast Program (SBP) menu on the day of and the day after they are offered on the NSLP or SBP menu), as well as food items and beverages from vending machines, from school stores, or as fund-raisers, including those operated by student clubs and organizations, parent groups, or boosters clubs.

E. All foods offered on the school campus during the school day shall comply with the current USDA Dietary Guidelines for Americans, including competitive foods that are available to students a la carte in the dining area, as classroom snacks, or from vending machines.

[DRAFTING NOTE: THE FINAL RULES STATE THAT A POLICY MUST HAVE STANDARDS FOR FOOD AND BEVERAGES "PROVIDED" AT SCHOOL, SUCH AS PROVIDED FOR A CLASS PARTY OR AS A REWARD TO STUDENTS. THESE STANDARDS DO NOT HAVE TO MEET THE REQUIREMENTS IMPOSED ON FOOD SOLD AT SCHOOL. A DISTRICT CAN ADOPT THE SAME STANDARD AS FOR SOLD FOOD OR ESTABLISH ITS OWN STANDARDS AS LONG AS IT HAS SOMETHING IN PLACE FOR FOOD PROVIDED IN SCHOOL OTHER THAN THROUGH SALE. THIS DOES NOT APPLY TO FOOD BROUGHT IN FOR INDIVIDUAL CONSUMPTION, I.E., A SACK LUNCH.]

F. All food and beverages that are provided, other than through sale, on the school campus during the school day (which may include classroom snacks, for classroom parties, and at holiday celebrations) shall comply with the
[x] food and beverage standards approved by the Superintendent.

(x) The food service program will provide all students affordable access to the varied and nutritious foods they need to be healthy and to learn well.

(X) The food service program shall be administered by a qualified nutrition professional.

(X) Continuing professional development shall be provided for all staff of the food service program.

The Board designates the **(X)** Superintendent as the individual(s) charged with operational responsibility for verifying that the District meets the goals established in this policy.

The Superintendent will appoint a District wellness committee that includes the opportunity for parents, students, representatives of the school food authority, educational staff (including health and physical education teachers), mental health and social services staff, school health professionals, members of the public and school administrators to participate in development, implementation, evaluation and periodic update of the wellness policy. The Wellness Committee shall be an ad hoc committee with members recruited and chosen annually.

The Wellness Committee shall be responsible for:

B. review of the District's wellness policy;

C. presentation of the wellness policy to the school board for approval;

Before the end of each school year the Wellness Committee shall recommend to the Superintendent any revisions to the policy it deems necessary and/or appropriate. In its review, the Wellness Committee shall consider evidence-based strategies in determining its recommendations.

The Superintendent shall report annually to the Board on the progress of the Wellness Committee and on its evaluation of policy implementation and areas for improvement, including status of compliance by individual schools and progress made in attaining goals of policy.

The Superintendent is also responsible for informing the public, including parents, students and community members, on the content and implementation of this policy. In order to inform the public, the Superintendent will:

(X) distribute information at the beginning of the school year to families of school children;

(X) include information in the student handbook;

and post the policy on the District's website, including the Wellness Committee's assessment of the implementation of the policy.

The District should assess the Wellness Policy at least once every three (3) years on the extent to which schools in the District are in compliance with the District policy, the extent to which the District policy compares to model wellness policies, and the progress made in attaining the goals of the District Wellness Policy. The assessment shall be made available to the public

(X) on the School District's web site.

42 U.S.C. 1751, Sec. 204
42 U.S.C. 1771
7 C.F.R. Parts 210 and 220