

Series 4000: District Employment

4100 Employee Rights and Responsibilities

4101 Non-Discrimination

A. Equal Employment Opportunity

The District is committed to equal employment opportunity and compliance with federal, state, and local laws that prohibit workplace Unlawful Discrimination, including unlawful harassment and Retaliation, based on any protected class or activity. This Policy applies to all aspects of employment, including recruiting, advertising, hiring, training, job placement, evaluation, classification, promotion, transfer, work assignment, compensation, benefits, discipline, demotion, termination, reduction in force, recall, and any other term or condition of employment.

This Policy prohibits discrimination against employees or applicants for employment based on the following protected classes: race, color, national origin, ethnicity, religion, sex, sexual orientation, gender identity or expression, pregnancy, height, weight, marital status, age, disability, genetic information, veteran status, military service, or any other legally protected class. This Policy also prohibits Retaliation based on a protected activity.

The District prohibits unlawful employment discrimination as required by applicable civil rights statutes, including:

- Title VI of the Civil Rights Act of 1964, which prohibits discrimination based on race, color, religion, or national origin;
- Title VII of the Civil Rights Act of 1964, which prohibits discrimination based on race, color, religion, sex (including gender identity, and sexual orientation), or national origin;
- Title IX of the Education Amendments of 1972, which prohibits discrimination based on sex;
- Age Discrimination in Employment Act of 1967 (ADEA), which prohibits discrimination based on age as to persons who are at least 40 years old;
- Equal Pay Act of 1963, which prohibits sex discrimination in payment of wages for persons performing substantially equal work in the same establishment;
- Section 504 of the Rehabilitation Act of 1973 (Section 504), which prohibits discrimination based on disability;

- Americans with Disabilities Act of 1990 (ADA), which prohibits discrimination against qualified persons with disabilities in employment, public service, public accommodations, and telecommunications;
- Pregnancy Discrimination Act of 1978, which prohibits discrimination based on pregnancy, childbirth, or related medical conditions;
- Pregnant Workers Fairness Act (PWFA), which requires covered employers to provide reasonable accommodations to a worker's known limitations related to pregnancy, childbirth, or related medical conditions, unless the accommodation will cause an undue hardship;
- Genetic Information Non-Discrimination Act of 2008 (GINA), which prohibits discrimination based on genetic information as to health insurance and employment;
- Michigan Elliott-Larsen Civil Rights Act of 1976 (ELCRA), which prohibits discrimination based on race, color, national origin, age, sex, pregnancy, sexual orientation, gender identity or expression, religion, height, weight, or marital status;
- Michigan Persons with Disabilities Civil Rights Act of 1976 (MPDCRA), which prohibits discrimination against qualified persons based on disability that is unrelated to that person's ability to perform the duties of a particular position or genetic information; and
- Michigan Equal Pay Act, which prohibits discriminatory wage practices based on sex.

The District also complies with and prohibits employment action that violates the following statutes:

- Family and Medical Leave Act of 1993 (FMLA), which requires covered employers to provide up to 12 work weeks of unpaid, job-protected leave to eligible employees for certain family, military, and medical reasons, and up to 26 work weeks to care for a covered service member with a serious injury or illness;
- Earned Sick Time Act (ESTA), which provides eligible employees with earned sick time that may be used for certain reasons;
- Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA), which provides job protection and reemployment rights to individuals who voluntarily or involuntarily leave employment to undertake military service, including military reservists and National Guard members called to duty;

- Public Employment Relations Act of 1947 (PERA), which prohibits a public employer from discriminating against an employee based on membership or non-membership in a labor organization;
- Fair Labor Standards Act of 1938 (FLSA), which establishes minimum wage, overtime pay, record keeping, and youth employment standards affecting employees; and
- Michigan Whistleblower Protection Act of 1980, which protects employees who report a violation or suspected violation of state, local, or federal law and employees who participate in hearings, investigations, or court actions.

B. Reporting Requirements

Any employee who believes he/she has been subjected to behavior that violates this Policy is encouraged to file a complaint promptly with a supervisor. A complaint implicating an individual's civil rights will be investigated pursuant to the procedures outlined in Policy 4104 and 3115-3115H. A complaint alleging Title IX sexual harassment will be investigated pursuant to the procedures outlined in Policy 3118.

Employees with questions about compliance with this Policy and applicable laws should contact the Superintendent or the Employment Compliance Officer(s) identified in Policy 3115B.

Board members, administrators, and supervisors must promptly report incidents of Unlawful Discrimination and Retaliation that he/she observes or about which he/she receives information.

Board members, administrators, or supervisors who receive a complaint alleging a violation of this Policy must promptly report the complaint, in writing, to the Employment Compliance Officer(s) identified in Policy 3115B.

A failure to comply with reporting requirements may result in discipline, including discharge.

C. Employment Discrimination Compliance Training

The District will train administrators, supervisors, and the Employment Compliance Officer(s) on how to address and investigate Unlawful Discrimination and Retaliation complaints.

The District may also provide Unlawful Discrimination and Retaliation training to Board members and employees.

Training may be provided by an outside entity or person approved by the District.

Legal authority: 20 USC 1681 et seq.; 29 USC 206 et seq., 701 et seq., 2601 et seq.; 38USC 4301 et seq.; 42 USC 2000d et seq., 2000e et seq., 2000ff et seq., 12101 et seq.; H.R. 2617-1626, 117th Cong. § 103(1) (signed into

law December 29, 2022); MCL 37.1101 et seq., 37.2101 et seq.; MCL 423.201 et seq.; MCL 750.556; 34 CFR 106.1 et seq.; MCL 408.934b, 408.961 et seq., *Mothering Justice v Attorney General*, 515 Mich 328 (2024)

Date adopted: August 15, 2022

Date revised: August 19, 2024

Date revised: February 17, 2025

Date revised: August 18, 2025

Date revised: July 20, 2026

Series 4000: District Employment

4100 Employee Rights and Responsibilities

4101 Non-Discrimination

A. Equal Employment Opportunity

The District is committed to equal employment opportunity and compliance with federal, state, and local laws that prohibit workplace Unlawful Discrimination, including unlawful harassment and Retaliation, based on any protected class or activity. This Policy applies to all aspects of employment, including recruiting, advertising, hiring, training, job placement, evaluation, classification, promotion, transfer, work assignment, compensation, benefits, discipline, demotion, termination, reduction in force, recall, and any other term or condition of employment.

This Policy prohibits discrimination against employees or applicants for employment based on the following protected classes: race, color, national origin, ethnicity, religion, sex, sexual orientation, gender identity or expression, pregnancy, height, weight, marital status, age, disability, genetic information, veteran status, military service, or any other legally protected class. This Policy also prohibits Retaliation based on a protected activity.

The District prohibits unlawful employment discrimination as required by applicable civil rights statutes, including:

- Title VI of the Civil Rights Act of 1964, which prohibits discrimination based on race, color, religion, or national origin;
- Title VII of the Civil Rights Act of 1964, which prohibits discrimination based on race, color, religion, sex (including gender identity, and sexual orientation), or national origin;
- Title IX of the Education Amendments of 1972, which prohibits discrimination based on sex;
- Age Discrimination in Employment Act of 1967 (ADEA), which prohibits discrimination based on age as to persons who are at least 40 years old;
- Equal Pay Act of 1963, which prohibits sex discrimination in payment of wages for persons performing substantially equal work in the same establishment;
- Section 504 of the Rehabilitation Act of 1973 (Section 504), which prohibits discrimination based on disability;



- Americans with Disabilities Act of 1990 (ADA), which prohibits discrimination against qualified persons with disabilities in employment, public service, public accommodations, and telecommunications;
- Pregnancy Discrimination Act of 1978, which prohibits discrimination based on pregnancy, childbirth, or related medical conditions;
- Pregnant Workers Fairness Act (PWFA), which requires covered employers to provide reasonable accommodations to a worker's known limitations related to pregnancy, childbirth, or related medical conditions, unless the accommodation will cause an undue hardship;
- Genetic Information Non-Discrimination Act of 2008 (GINA), which prohibits discrimination based on genetic information as to health insurance and employment;
- Michigan Elliott-Larsen Civil Rights Act of 1976 (ELCRA), which prohibits discrimination based on race, color, national origin, age, sex, pregnancy, sexual orientation, gender identity or expression, religion, height, weight, or marital status;
- Michigan Persons with Disabilities Civil Rights Act of 1976 (MPDCRA), which prohibits discrimination against qualified persons based on disability that is unrelated to that person's ability to perform the duties of a particular position or genetic information; and
- Michigan Equal Pay Act, which prohibits discriminatory wage practices based on sex.

The District also complies with and prohibits employment action that violates the following statutes:

- Family and Medical Leave Act of 1993 (FMLA), which requires covered employers to provide up to 12 work weeks of unpaid, job-protected leave to eligible employees for certain family, military, and medical reasons, and up to 26 work weeks to care for a covered service member with a serious injury or illness;
- Earned Sick Time Act (ESTA), which provides eligible employees with earned sick time that may be used for certain reasons;
- Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA), which provides job protection and reemployment rights to individuals who voluntarily or involuntarily leave employment to undertake military service, including military reservists and National Guard members called to duty;

- Public Employment Relations Act of 1947 (PERA), which prohibits a public employer from discriminating against an employee based on membership or non-membership in a labor organization;
- Fair Labor Standards Act of 1938 (FLSA), which establishes minimum wage, overtime pay, record keeping, and youth employment standards affecting employees; and
- Michigan Whistleblower Protection Act of 1980, which protects employees who report a violation or suspected violation of state, local, or federal law and employees who participate in hearings, investigations, or court actions.

B. Reporting Requirements

Any employee who believes he/she has been subjected to behavior that violates this Policy is encouraged to file a complaint promptly with a supervisor. A complaint implicating an individual's civil rights will be investigated pursuant to the procedures outlined in Policy 4104 and 3115-3115H. A complaint alleging Title IX sexual harassment will be investigated pursuant to the procedures outlined in Policy 3118.

Employees with questions about compliance with this Policy and applicable laws should contact the Superintendent or the Employment Compliance Officer(s) identified in Policy 3115B.

Board members, administrators, and supervisors must promptly report incidents of Unlawful Discrimination and Retaliation that he/she observes or about which he/she receives information.

Board members, administrators, or supervisors who receive a complaint alleging a violation of this Policy must promptly report the complaint, in writing, to the Employment Compliance Officer(s) identified in Policy 3115B.

A failure to comply with reporting requirements may result in discipline, including discharge.

C. Employment Discrimination Compliance Training

The District will train administrators, supervisors, and the Employment Compliance Officer(s) on how to address and investigate Unlawful Discrimination and Retaliation complaints.

The District may also provide Unlawful Discrimination and Retaliation training to Board members and employees.

Training may be provided by an outside entity or person approved by the District.

Legal authority: 20 USC 1681 et seq.; 29 USC 206 et seq., 701 et seq., 2601 et seq.; 38 USC 4301 et seq.; 42 USC 2000d et seq., 2000e et seq., 2000ff et seq., 12101 et seq.; H.R. 2617-1626, 117th Cong. § 103(1) (signed into

law December 29, 2022); MCL 37.1101 et seq., 37.2101 et seq.; MCL 423.201 et seq.; MCL 750.556; 34 CFR 106.1 et seq.; MCL 408.934b, 408.961 et seq., *Mothering Justice v Attorney General*, [2024 Mich LEXIS 1454](#) [515 Mich 328](#) (July 31, 2024)

Date adopted:

Date revised:

Series 4000: District Employment

4100 Employee Rights and Responsibilities

4104 Employment Complaint Procedure for Allegations Implicating Civil Rights

This employment complaint procedure for allegations implicating an employee's civil rights is designed to facilitate: (1) prompt notification of alleged Unlawful Discrimination, including unlawful harassment and Retaliation; (2) a prompt and thorough investigation of good faith allegations; and (3) the implementation of appropriate corrective action, if necessary, to eliminate verified Unlawful Discrimination, harassment, and Retaliation from the workplace.

A. Initiating a Complaint

1. A Board member, employee, or employment applicant who believes he/she has been the subject of Unlawful Discrimination, harassment or Retaliation, must timely file a complaint, preferably within 10 business days of the alleged or suspected violation or when the reporter obtained knowledge of the alleged or suspected violation, with the Employment Compliance Officer or applicable coordinator listed in Policy 3115B.
2. A complaint of Unlawful Discrimination, including harassment or Retaliation, may be made verbally or in writing. The complaint will be memorialized on Form 3115-F-1.
3. A complaint alleging Title IX sexual harassment must be submitted in writing and signed by the complainant. Policy 3118 governs the Title IX sexual harassment complaint procedures.

B. Investigation Procedures

A written or verbal report (including an anonymous report) of Unlawful Discrimination, including harassment or Retaliation, will be investigated promptly and thoroughly using the Grievance Procedure outlined in Policy 3115E, unless the Complaint is dismissed pursuant to Policy 3115F or informal resolution is reached pursuant to Policy 3115D.

A complaint alleging Title IX sexual harassment will be investigated pursuant to the process set forth in Policy 3118.

C. Reports to State or Federal Administrative Agencies

Any person who believes that he/she was the victim of Unlawful Discrimination, including unlawful harassment or Retaliation, may file a complaint with the Michigan Department of Civil Rights (MDCR) or the Equal Employment Opportunity Commission (EEOC) at any time:

Michigan Department of Civil Rights

Telephone: 1-800-482-3604
Email: MDCRServiceCenter@michigan.gov
Public Portal: <https://www.michigan.gov/mdcr/public-portal>

Equal Employment Opportunity Commission Patrick V. McNamara Building
477 Michigan Avenue - Room 865
Detroit, MI 48226
Phone: 800-669-4000
Fax: 313-226-4610
TTY: 800-669-6820
ASL Video: 844-234-5122
Public Portal: <https://publicportal.eeoc.gov/portal/>
Email: info@eeoc.gov

An agency complaint may be filed before, during, or after a complaint is filed with the District, or a person may forego filing a complaint with the District and rely solely on the MDCR or EEOC. The District recommends that a person who has been subjected to Unlawful Discrimination, including unlawful harassment or Retaliation, also file a complaint with the District to ensure that the District can take steps to prevent further Unlawful Discrimination, including unlawful harassment or Retaliation, and to discipline the Respondent, if appropriate. The MDCR and EEOC do not serve as an appellate body for District decisions. An investigation by the MDCR or EEOC will occur separately from any District investigation.

Legal authority: U.S. CONST. amend. XIV; 20 USC 1681 et seq.; 29 USC 701 et seq.; 42 USC 2000d et seq., 2000e et seq., 2000ff et seq., 6101 et seq., 12101 et seq.; 29 CFR 1630; 34 CFR 104, 106.1, et seq.; MCL 15.261 et seq.; MCL 37.1101 et seq., 37.2101 et seq.

Date adopted: August 15, 2022

Date revised: August 19, 2024

Date revised: February 17, 2025

Date revised: July 20, 2026

Series 4000: District Employment

4100 Employee Rights and Responsibilities

4104 Employment Complaint Procedure for Allegations Implicating Civil Rights

This employment complaint procedure for allegations implicating an employee's civil rights is designed to facilitate: (1) prompt notification of alleged Unlawful Discrimination, including unlawful harassment and Retaliation; (2) a prompt and thorough investigation of good faith allegations; and (3) the implementation of appropriate corrective action, if necessary, to eliminate verified Unlawful Discrimination, harassment, and Retaliation from the workplace.

A. Initiating a Complaint

1. A Board member, employee, or employment applicant who believes he/she has been the subject of Unlawful Discrimination, harassment or Retaliation, must timely file a complaint, preferably within 10 business days of the alleged or suspected violation or when the reporter obtained knowledge of the alleged or suspected violation, with the Employment Compliance Officer or applicable coordinator listed in Policy 3115B.
2. A complaint of Unlawful Discrimination, including harassment or Retaliation, may be made verbally or in writing. The complaint will be memorialized on Form 3115-F-1.
3. A complaint alleging Title IX sexual harassment must be submitted in writing and signed by the complainant. Policy 3118 governs the Title IX sexual harassment complaint procedures.

B. Investigation Procedures

A written or verbal report (including an anonymous report) of Unlawful Discrimination, including harassment or Retaliation, will be investigated promptly and thoroughly using the Grievance Procedure outlined in Policy 3115E, unless the Complaint is dismissed pursuant to Policy 3115F or informal resolution is reached pursuant to Policy 3115D.

A complaint alleging Title IX sexual harassment will be investigated pursuant to the process set forth in Policy 3118.

C. Reports to State or Federal Administrative Agencies

Any person who believes that he/she was the victim of Unlawful Discrimination, including unlawful harassment or Retaliation, may file a complaint with the Michigan Department of Civil Rights (MDCR) or the Equal Employment Opportunity Commission (EEOC) at any time:

Michigan Department of Civil Rights ~~Capitol Tower Building~~

Telephone: 1-800-482-3604
Email: MDCRServiceCenter@michigan.gov
Public Portal: <https://www.michigan.gov/mdcr/public-portal>
110 W. Michigan Avenue, Suite 800
Lansing, MI 48933
Phone: 517-335-3165
Fax: 517-241-0546
TTY: 517-241-1965
Email: MDCR-INFO@michigan.gov

Equal Employment Opportunity Commission Patrick V. McNamara Building
477 Michigan Avenue - Room 865
Detroit, MI 48226
Phone: 800-669-4000
Fax: 313-226-4610
TTY: 800-669-6820
ASL Video: 844-234-5122
Public Portal: <https://publicportal.eeoc.gov/portal/>
Email: info@eeoc.gov

Field Code Changed

An agency complaint may be filed before, during, or after a complaint is filed with the District, or a person may forego filing a complaint with the District and rely solely on the MDCR or EEOC. The District recommends that a person who has been subjected to Unlawful Discrimination, including unlawful harassment or Retaliation, also file a complaint with the District to ensure that the District can take steps to prevent further Unlawful Discrimination, including unlawful harassment or Retaliation, and to discipline the Respondent, if appropriate. The MDCR and EEOC do not serve as an appellate body for District decisions. An investigation by the MDCR or EEOC will occur separately from any District investigation.

Legal authority: U.S. CONST. amend. XIV; 20 USC 1681 et seq.; 29 USC 701 et seq.; 42 USC 2000d et seq., 2000e et seq., 2000ff et seq., 6101 et seq., 12101 et seq.; 29 CFR 1630; 34 CFR 104, 106.1, et seq.; MCL 15.261 et seq.; MCL 37.1101 et seq., 37.2101 et seq.

Date adopted:

Date revised:

Series 4000: District Employment

4100 Employee Rights and Responsibilities

4113 Michigan Earned Sick Time Act (ESTA)

A. General

Eligible employees will accrue paid leave as provided by the ESTA. Applicable provisions of a collective bargaining agreement, individual employment contract, or handbook remain in place and may provide additional paid leave time that is not provided by the ESTA.

Unless otherwise agreed with union representation, the ESTA does not apply to employees subject to a conflicting collective bargaining agreement in effect on February 21, 2025, until the collective bargaining agreement expires.

The ESTA does not apply to an employee subject to a conflicting individual employment contract in effect on February 21, 2025, until that contract expires, if all of the following are satisfied:

- the District and the employee signed the contract on or before December 31, 2024;
- the contract is effective for not longer than 3 years; and
- the District notified the Michigan Department of Labor and Economic Opportunity (LEO) of the contract.

B. Definitions

1. "ESTA benefit year" means the 12-month period from July 1 to June 30.
2. "Eligible employee" means an employee engaged in service to the District. The following, however, are not eligible employees:
 - a. an unpaid trainee or unpaid intern;
 - b. a person employed in accordance with the Michigan Youth Employment Standards Act, MCL 409.101, *et seq*; or
 - c. positions when the employee may schedule their own working hours as approved by the Superintendent or designee. For those approved positions, the District will not take adverse personnel action for failure to schedule a minimum amount of working hours.

If a collective bargaining agreement or contract meets the requirements in Section A above, then an employee covered by that contract is not an eligible employee until the contract expires.

3. "Family member" is defined as:

- a. biological, adopted, or foster child, stepchild or legal ward, a child of a domestic partner, or a child to whom the eligible employee stands *in loco parentis*;
- b. biological parent, foster parent, stepparent, or adoptive parent or legal guardian of an eligible employee or an eligible employee's spouse (under the laws of any state) or domestic partner or a person who stood *in loco parentis* when the eligible employee was a minor child;
- c. an individual to whom the eligible employee is legally married under the laws of any state or a domestic partner;
- d. grandparent, grandchild, and biological, foster, or adopted sibling;
- e. an individual related by blood; or
- f. an individual whose close association with the eligible employee is the equivalent of a family relationship.

4. "Earned sick time" means paid leave as allowed by the ESTA.

5. All other ESTA-defined terms apply to this Policy.

C. Wait Period and Leave Reinstatement Upon Re-Employment

A newly hired eligible employee may not use accrued earned sick time until 120 calendar days after the employee's start date, unless otherwise provided in a collective bargaining agreement, individual employment contract, employee handbook, or the ESTA.

Upon discharge or other separation from employment, an employee automatically loses accrued earned sick time unless the employee is rehired by the District within 2 months of the separation.

Accrued earned sick time that is not used before an employee's separation from employment will have no monetary value. If an employee separates from employment and is rehired by the District not more than two (2) months after separation, the District will reinstate previously accrued and unused earned sick time and allow the employee to use that earned sick time and accrue additional earned sick time upon reinstatement. This paragraph does not apply if the District paid the employee the value of the employee's unused accrued earned sick time at the time of separation.

D. ESTA Leave Accrual and Frontloading

1. Leave Accrual

Unless the District frontloads earned sick time under Section D(2), an eligible employee begins accruing earned sick time on February 21, 2025 or the employee's start date, whichever is later.

An eligible employee will accrue 1 hour of earned sick time for every 30 hours worked, but the eligible employee may only use up to 72 hours of earned sick time in a single ESTA benefit year. An FLSA-exempt eligible employee is assumed to work 40 hours per workweek unless the employee's normal workweek is less than 40 hours.

Up to 72 hours of unused accrued earned sick time will carry over from ESTA benefit year to ESTA benefit year.

2. Frontloading Leave

For each ESTA benefit year, the District may frontload earned sick time consistent with this policy, a collective bargaining agreement, or individual employment contract.

If frontloading, the District will grant a full-time eligible employee 72 hours of earned sick time at the beginning of an ESTA benefit year. For a part-time eligible employee, the District will provide the employee with:

- a written notice of how many hours the employee is expected to work during the ESTA benefit year at the time of hire;
- an amount of earned sick time at the beginning of the ESTA benefit year that is proportional to the earned sick time the employee would accrue if the employee worked all the hours in that written notice; and
- 1 hour of earned sick time for every 30 hours worked after the employee exceeds the work hours in that written notice.

Frontloaded earned sick time will not carry over from one ESTA benefit year to the next unless authorized in the applicable collective bargaining agreement, individual employment contract, or handbook.

3. Compliance Presumption

The District is in compliance with this Section D if it:

- provides an eligible employee with paid time off in at least the same amounts of time off described in the ESTA that may be used for ESTA purposes or any other approved purpose, with the time used for an ESTA purpose being subject to the ESTA; or
- is a signatory to a collective bargaining agreement that requires contributions to a multiemployer plan under the Employee Retirement Income Security Act, subject to certain conditions.

E. Additional Absences

Additional absences, above and beyond earned sick time under the ESTA, are governed by an applicable collective bargaining agreement, individual employment contract, or Board Policy.

F. Permissible Uses

An eligible employee may use earned sick time for the following reasons:

1. the employee's mental or physical illness, injury, or health condition; medical diagnosis, care, or treatment of the employee's mental or physical illness, injury, or health condition; or preventative medical care for the employee;
2. for the employee's family member's mental or physical illness, injury, or health condition, medical diagnosis, care, or treatment of the employee's family member's mental or physical illness, injury, or health condition or preventative medical care for a family member of the employee;
3. if the employee or the employee's family member is a victim of domestic violence or sexual assault, for medical care or psychological or other counseling for physical or psychological injury or disability, to obtain services from a victim services organization, to relocate due to domestic violence or sexual assault, to obtain legal services, or to participate in any civil or criminal proceedings related to or resulting from the domestic violence or sexual assault;
4. for meetings at a child's school or place of care related to the child's health or disability, or the effects of domestic violence or sexual assault on the child; or
5. for closure of the employee's place of business by order of a public official due to a public health emergency, for an employee's need to care for a child whose school or place of care has been closed by order of a public official due to a public health emergency, or when it has been determined by the health authorities having jurisdiction or by a health care provider that the employee's or employee's family member's presence in the community would jeopardize the health of others because of the employee's or family member's exposure to a communicable disease, whether or not the employee or family member has actually contracted the communicable disease.

G. Use of Earned Sick Time

If the eligible employee's need to use leave is foreseeable, the employee must provide notice to the District of the employee's intent to use earned sick time at least 7 days prior to the date leave is to begin. If the eligible employee's need to use leave is not foreseeable, the employee must provide notice to the District of the employee's intent to use earned sick time as soon as practicable. For leave of more than 3 consecutive days, upon District request, the eligible employee must provide the District – within 15 days after the request – reasonable documentation that earned sick time was used for an ESTA purpose. The District will be

responsible for paying the eligible employee's costs in obtaining the requested documentation.

In cases of domestic violence or sexual assault, reasonable documentation includes any of the following:

- a police report indicating that the employee or the employee's family member was a victim of domestic violence or sexual assault;
- a signed statement from a victim and witness advocate affirming that the employee or the employee's family member is receiving services from a victim services organization; or
- a court document indicating that the employee or the employee's family member is involved in legal action related to domestic violence or sexual assault.

All health, sexual assault, and domestic violence information and documentation received from an employee about earned sick time remains confidential and will not be disclosed, except to the employee, with the employee's written permission, or as and to the extent required by law.

Failure to comply with notice procedures or document requests to support the use of earned sick time, or using earned sick time for a non-permissible use, may result in discipline, including discharge.

Unless otherwise provided in an employee's collective bargaining agreement, individual employment contract, or handbook:

- earned sick time must be used in hourly increments (or the smallest applicable increment that the District uses to account for absences of use of other time); and
- an employee using earned sick time will not receive overtime pay, holiday pay, or bonuses for the earned sick time.

H. Notice and Recordkeeping

The District will:

1. provide an ESTA notice created by LEO to each eligible employee at hire (see 4113-F-1);
2. display in a conspicuous location in each of its buildings the ESTA poster created by LEO; and
3. retain for not less than 3 years records documenting hours worked and earned sick time taken by eligible employees.

Legal authority: MCL 408.934b, 408.961 et seq., *Mothering Justice v Attorney General*,
515 Mich 328 (2024)

Date adopted: February 17, 2025

Date revised: March 17, 2025

Date revised: July 20, 2026



Series 4000: District Employment

4100 Employee Rights and Responsibilities

4113 **Michigan Earned Sick Time Act (ESTA)** [Required for Districts with More Than 10 Employees] [Note: If the District has 10 or fewer employees, please contact the Thrun Board Policy Administrator to receive a different version of this ESTA policy.]

A. General

Eligible employees will accrue paid leave as provided by the ESTA. Applicable provisions of a collective bargaining agreement, individual employment contract, or handbook remain in place and may provide additional paid leave time that is not provided by the ESTA.

Unless otherwise agreed with union representation, the ESTA does not apply to employees subject to a conflicting collective bargaining agreement in effect on February 21, 2025, until the collective bargaining agreement expires.

The ESTA does not apply to an employee subject to a conflicting individual employment contract in effect on February 21, 2025, until that contract expires, if all of the following are satisfied:

- the District and the employee signed the contract on or before December 31, 2024;
- the contract is effective for not longer than 3 years; and
- the District notified the Michigan Department of Labor and Economic Opportunity (LEO) of the contract.

B. Definitions

1. "ESTA benefit year" means the 12-month period from July 1 to June 30. [Optional: may adjust 12-month period]
2. "Eligible employee" means an employee engaged in service to the District. The following, however, are not eligible employees:
 - a. an unpaid trainee or unpaid intern;
 - b. a person employed in accordance with the Michigan Youth Employment Standards Act, MCL 409.101, *et seq*; or
 - c. positions when the employee may schedule their own working hours as approved by the Superintendent or designee. For those approved positions, the District will not take adverse personnel action for failure to schedule a minimum amount of working hours.

If a collective bargaining agreement or contract meets the requirements in Section A above, then an employee covered by that contract is not an eligible employee until the contract expires.

3. "Family member" is defined as:

- a. biological, adopted, or foster child, stepchild or legal ward, a child of a domestic partner, or a child to whom the eligible employee stands *in loco parentis*;
- b. biological parent, foster parent, stepparent, or adoptive parent or legal guardian of an eligible employee or an eligible employee's spouse (under the laws of any state) or domestic partner or a person who stood *in loco parentis* when the eligible employee was a minor child;
- c. an individual to whom the eligible employee is legally married under the laws of any state or a domestic partner;
- d. grandparent, grandchild, and biological, foster, or adopted sibling;
- e. an individual related by blood; or
- f. an individual whose close association with the eligible employee is the equivalent of a family relationship.

4. "Earned sick time" means paid leave as allowed by the ESTA.

5. All other ESTA-defined terms apply to this Policy.

C. Wait Period and Leave Reinstatement Upon Re-Employment

A newly hired eligible employee may not use accrued earned sick time until 120 calendar days after the employee's start date, unless otherwise provided in a collective bargaining agreement, individual employment contract, employee handbook, or the ESTA.

Upon discharge or other separation from employment, an employee automatically loses accrued earned sick time unless the employee is rehired by the District within 2 months of the separation.

Accrued earned sick time that is not used before an employee's separation from employment will have no monetary value. If an employee separates from employment and is rehired by the District not more than two (2) months after separation, the District will reinstate previously accrued and unused earned sick time and allow the employee to use that earned sick time and accrue additional earned sick time upon reinstatement. This paragraph does not apply if the District paid the employee the value of the employee's unused accrued earned sick time at the time of separation.

D. ESTA Leave Accrual and Frontloading

1. Leave Accrual

Unless the District frontloads earned sick time under Section D(2), an eligible employee begins accruing earned sick time on February 21, 2025 or the employee's start date, whichever is later.

An eligible employee will accrue 1 hour of earned sick time for every 30 hours worked, but the eligible employee may only use up to 72 hours of earned sick time in a single ESTA benefit year. An FLSA-exempt eligible employee is assumed to work 40 hours per workweek unless the employee's normal workweek is less than 40 hours.

Up to 72 hours of unused accrued earned sick time will carry over from ESTA benefit year to ESTA benefit year.

2. Frontloading Leave

For each ESTA benefit year, the District may frontload earned sick time consistent with this policy, a collective bargaining agreement, or individual employment contract.

If frontloading, the District will grant a full-time eligible employee 72 hours of earned sick time at the beginning of an ESTA benefit year. For a part-time eligible employee, the District will provide the employee with:

- a written notice of how many hours the employee is expected to work during the ESTA benefit year at the time of hire;
- an amount of earned sick time at the beginning of the ESTA benefit year that is proportional to the earned sick time the employee would accrue if the employee worked all the hours in that written notice; and
- 1 hour of earned sick time for every 30 hours worked after the employee exceeds the work hours in that written notice.

Frontloaded earned sick time will not carry over from one ESTA benefit year to the next unless authorized in the applicable collective bargaining agreement, individual employment contract, or handbook.

3. Compliance Presumption

The District is in compliance with this Section D if it:

- provides an eligible employee with paid time off in at least the same amounts of time off described in the ESTA that may be used for ESTA purposes or any other approved purpose, with the time used for an ESTA purpose being subject to the ESTA; or

- is a signatory to a collective bargaining agreement that requires contributions to a multiemployer plan under the Employee Retirement Income Security Act, subject to certain conditions.

E. Additional Absences

Additional absences, above and beyond earned sick time under the ESTA, are governed by an applicable collective bargaining agreement, individual employment contract, or Board Policy.

F. Permissible Uses

An eligible employee may use earned sick time for the following reasons:

1. the employee's mental or physical illness, injury, or health condition; medical diagnosis, care, or treatment of the employee's mental or physical illness, injury, or health condition; or preventative medical care for the employee;
2. for the employee's family member's mental or physical illness, injury, or health condition, medical diagnosis, care, or treatment of the employee's family member's mental or physical illness, injury, or health condition or preventative medical care for a family member of the employee;
3. if the employee or the employee's family member is a victim of domestic violence or sexual assault, for medical care or psychological or other counseling for physical or psychological injury or disability, to obtain services from a victim services organization, to relocate due to domestic violence or sexual assault, to obtain legal services, or to participate in any civil or criminal proceedings related to or resulting from the domestic violence or sexual assault;
4. for meetings at a child's school or place of care related to the child's health or disability, or the effects of domestic violence or sexual assault on the child; or
5. for closure of the employee's place of business by order of a public official due to a public health emergency, for an employee's need to care for a child whose school or place of care has been closed by order of a public official due to a public health emergency, or when it has been determined by the health authorities having jurisdiction or by a health care provider that the employee's or employee's family member's presence in the community would jeopardize the health of others because of the employee's or family member's exposure to a communicable disease, whether or not the employee or family member has actually contracted the communicable disease.

G. Use of Earned Sick Time

If the eligible employee's need to use leave is foreseeable, the employee must provide notice to the District of the employee's intent to use earned sick time at least 7 days prior to the date leave is to begin. If the eligible employee's need to

use leave is not foreseeable, the employee must provide notice to the District of the employee's intent to use earned sick time as soon as practicable. For leave of more than 3 consecutive days, upon District request, the eligible employee must provide the District – within 15 days after the request – reasonable documentation that earned sick time was used for an ESTA purpose. The District will be responsible for paying the eligible employee's costs in obtaining the requested documentation.

In cases of domestic violence or sexual assault, reasonable documentation includes any of the following:

- a police report indicating that the employee or the employee's family member was a victim of domestic violence or sexual assault;
- a signed statement from a victim and witness advocate affirming that the employee or the employee's family member is receiving services from a victim services organization; or
- a court document indicating that the employee or the employee's family member is involved in legal action related to domestic violence or sexual assault.

All health, sexual assault, and domestic violence information and documentation received from an employee about earned sick time remains confidential and will not be disclosed, except to the employee, with the employee's written permission, or as and to the extent required by law.

Failure to comply with notice procedures or document requests to support the use of earned sick time, or using earned sick time for a non-permissible use, may result in discipline, including discharge.

Unless otherwise provided in an employee's collective bargaining agreement, individual employment contract, or handbook:

- earned sick time must be used in [] [Note: Insert "hourly" or the smallest increment that the District uses to account for absences of use of other time] increments; and
- an employee using earned sick time will not receive overtime pay, holiday pay, or bonuses for the earned sick time.

H. Notice and Recordkeeping

The District will:

1. provide an ESTA notice created by LEO to each eligible employee at hire ~~or by March 23, 2025, whichever is later~~ (see 4113-F-1);
2. display in a conspicuous location in each of its buildings the ESTA poster created by LEO; and

3. retain for not less than 3 years records documenting hours worked and earned sick time taken by eligible employees.

Legal authority: MCL 408.934b, 408.961 et seq., *Mothering Justice v Attorney General*,
~~2024 Mich LEXIS 1454 (July 31, 2024)~~[515 Mich 328 \(2024\)](#)

Date adopted:

Date revised:



Series 4000: District Employment

4200 Employee Conduct and Ethics

4201 *Employee Ethics and Standards*

Employees must act professionally and model high standards of behavior at all times. Employees shall perform their respective duties and responsibilities in a professional manner, using appropriate judgment. Employees must maintain a standard of behavior that reflects positively on their status as District representatives in the community and is consistent with the Michigan Code of Educational Ethics, which is incorporated herein by reference. See:

https://www.michigan.gov/documents/mde/Code_of_Ethics_653130_7.pdf

If an employee is uncertain as to a potential course of conduct, the employee should seek advice from a supervisor before proceeding.

A. Employee Ethical Conduct

Employees must exercise objectively sound and professional judgment when engaging with students, Parents, colleagues, administrators, Board members, and community members. This standard extends to employee conduct on and off school property. Ethical behavior generally includes, but is not limited to:

1. supporting the physical and emotional welfare and safety of students, Parents, colleagues, administrators, Board members, and community members;
2. complying with federal and state law;
3. competently and appropriately performing duties and responsibilities for which the employee is trained or assigned;
4. assigning tasks to personnel who are qualified and hired to perform the assigned task;
5. refraining from unlawful discrimination, including unlawful harassment, and retaliation as defined by Policy;
6. immediately reporting suspected child abuse or neglect;
7. immediately reporting reasonable cause to believe or suspect abuse, neglect, or exploitation of a vulnerable adult;
8. maintaining confidential information, including student, medical, personnel, financial, and security information, as protected by statute;
9. appropriately using District funds, resources, and technology;
10. maintaining consistent and reliable work attendance, unless excused by the employee's supervisor or the Superintendent or designee, as applicable;

11. engaging in activities or behaviors that enhance the operational and instructional environment;
12. professionally communicating with students, Parents, colleagues, Board members, and community members, including through electronic means;
13. completing time and effort reporting under 4201-AG;
14. abiding by professional, ethical, and licensing standards established by relevant governmental agencies, professional licensing boards, and professional associations, including the Michigan State Board of Education; and
15. self-reporting a criminal charge and plea or conviction, as required by law.

B. Conflict of Interest

Employees shall perform their duties and responsibilities free from a prohibited conflict of interest, unless authorized by the Board or designee. Prohibited conflicts of interest include, but are not limited to:

1. soliciting or accepting anything of value (such as a gift, loan, contribution, or reward), other than compensation received from the District in exchange for services provided to the District, that would influence the employee's judgment when performing the employee's duties;
2. using public funds to purchase alcoholic beverages, jewelry, gifts, fees for golf, or any item the purchase or possession of which is illegal, except as consistent with and permitted by Policy 3205 and Revised School Code Section 1814;
3. using or authorizing the use of the employee's public employment or any confidential information received through public employment to obtain personal, professional, political, or financial gain other than compensation received from the District in exchange for services provided to the District for the employee or a member of the employee's immediate family, or a business with which the employee is associated;
4. using or authorizing the use of District personnel, resources, property, or funds under the employee's care and control other than in accordance with prescribed constitutional, statutory, and regulatory procedures, or using those items for personal, professional, political, or financial gain;
5. providing private services, lessons, tutoring, or coaching for students assigned to the employee for additional remuneration, except as permitted by Policy 4214;
6. engaging in any activity of a sexual or romantic nature with another employee(s) or contractor(s) that the employee supervises, unless the individuals are engaged to be married, married, or cohabitating;

7. engaging in any activity of a sexual or romantic nature on school property or at school-sponsored events;
8. directly or indirectly supervising, making, or contributing to an employment decision pertaining to a relative or significant other, or relative of a relative or significant other (as defined by Policy 4213);
9. engaging in any other activity that promotes an employee's financial and pecuniary interests over those of the District; and
10. entering into a proposed contract in which an administrator has a substantial conflict of interest (for Board members, see Policy 2301). Employees shall comply with the disclosure requirements in Policy 2301E(1).

C. Student Fraternization

Employees must establish and maintain professional boundaries with students, including while using personal or District technology. Employees are prohibited from direct or indirect interactions with students that do not reasonably relate to an educational purpose. Employees will behave at all times in a manner supportive of the best interests of students and the District.

Conduct identified below constitutes unprofessional conduct, subjecting the employee to discipline, including discharge, absent express Board or designee authorization. The following list illustrates prohibited behavior involving students but does not describe every kind of prohibited behavior:

1. communicating about alcohol use, drug use, or sexual activity when the discussion is not appropriately related to a specific aspect of the curriculum or the employee's duties;
2. providing drugs, alcohol, tobacco, e-cigarettes, or other items students cannot possess under the District's Student Code of Conduct;
3. commenting about matters involving sex, using double entendre, or making sexually suggestive remarks with no appropriate educational purpose;
4. displaying sexually inappropriate images, materials, or objects;
5. offering or soliciting sexual advice, whether written, verbal, or physical;
6. engaging in any activity of a sexual or romantic nature, including following graduation where the relationship arises out of an employee-student relationship;
7. inappropriate kissing;
8. inappropriately intruding on a student's personal space, such as by touching unnecessarily, moving too close, or staring at a portion of the student's body;

9. communicating directly or indirectly (e.g., by phone, email, text messaging, or social media) on a matter that does not pertain to school without first obtaining the express permission of the student's Parent and a District administrator. Electronic communications with students generally are to be sent simultaneously to multiple recipients and not just to one student except when the communication is clearly school related and inappropriate for persons other than the individual student to receive (e.g., grades);
10. permitting a specific student to engage in conduct that is not permitted or tolerated from other students;
11. inappropriately discussing with a student the student's personal issues or problems that should normally be discussed with a Parent or counselor unless the employee is the student's family member;
12. inappropriately giving a student a personal gift;
13. allowing a student to live in the employee's residence without first obtaining the express permission of the student's Parent unless the student is the employee's family member, a foreign exchange student placed with the employee, or if the employee serves as the student's foster parent or legal guardian;
14. giving a student a ride in the employee's vehicle without appropriate authorization;
15. taking a student on an activity outside of school without first obtaining the express permission of the student's Parent and a District administrator;
16. inviting a student to the employee's home or residence without first obtaining the express permission of the student's Parent;
17. going to a student's home when the student's Parent or an adult chaperone is not present unless the employee is the student's family member; or
18. engaging in any other conduct which undermines the special position of trust and authority between a District employee and a student.

D. Abuse and Neglect

1. Children: An employee who suspects child abuse or neglect must: (a) immediately contact Children's Protective Services (CPS), (b) file an appropriate report with that agency as required by the Child Protection Law and Policy 4202, and (c) notify the Superintendent or designee and the building principal or supervisor that the report has been filed.

An employee should consult with their immediate supervisor about their duty to cooperate with CPS investigations or to disclose student records to CPS.

2. Vulnerable Adults: An employee who has reasonable cause to believe or suspect abuse, neglect, or exploitation of a vulnerable adult must: (a)

immediately report the matter to Adult Protective Services (APS) consistent with Michigan's Social Welfare Act and Policy 4202 and (b) notify the Superintendent or designee and the building principal or supervisor that the report has been filed.

A reporter's identity will remain confidential unless disclosure is authorized by the reporter's consent or by court order.

An employee should consult with their immediate supervisor about their duty to cooperate with APS investigations or to disclose student records to APS.

Legal authority: MCL 380.11a, 380.601a, 380.634, 380.1308a, 380.1814; MCL 722.621 et seq.; MCL 400.11a.

Date adopted: August 15, 2022

Date revised: August 19, 2024

Date revised: July 20, 2026

Series 4000: District Employment

4200 Employee Conduct and Ethics

4201 Employee Ethics and Standards

Employees must act professionally and model high standards of behavior at all times. Employees shall perform their respective duties and responsibilities in a professional manner, using appropriate judgment. Employees must maintain a standard of behavior that reflects positively on their status as District representatives in the community and is consistent with the Michigan Code of Educational Ethics, which is incorporated herein by reference. See:

https://www.michigan.gov/documents/mde/Code_of_Ethics_653130_7.pdf

If an employee is uncertain as to a potential course of conduct, the employee should seek advice from a supervisor before proceeding.

A. Employee Ethical Conduct

Employees must exercise objectively sound and professional judgment when engaging with students, Parents, colleagues, administrators, Board members, and community members. This standard extends to employee conduct on and off school property. Ethical behavior generally includes, but is not limited to:

1. supporting the physical and emotional welfare and safety of students, Parents, colleagues, administrators, Board members, and community members;
2. complying with federal and state law;
3. competently and appropriately performing duties and responsibilities for which the employee is trained or assigned;
4. assigning tasks to personnel who are qualified and hired to perform the assigned task;
5. refraining from unlawful discrimination, including unlawful harassment, and retaliation as defined by Policy;
6. immediately reporting suspected child abuse or neglect;
7. immediately reporting reasonable cause to believe or suspect abuse, neglect, or exploitation of a vulnerable adult;
8. maintaining confidential information, including student, medical, personnel, financial, and security information, as protected by statute;
9. appropriately using District funds, resources, and technology;
10. maintaining consistent and reliable work attendance, unless excused by the employee's supervisor or the Superintendent or designee, as applicable;

11. engaging in activities or behaviors that enhance the operational and instructional environment;
12. professionally communicating with students, Parents, colleagues, Board members, and community members, including through electronic means;
13. completing time and effort reporting under 4201-AG;
14. abiding by professional, ethical, and licensing standards established by relevant governmental agencies, professional licensing boards, and professional associations, including the Michigan State Board of Education; and
15. self-reporting a criminal charge and plea or conviction, as required by law.

B. Conflict of Interest

Employees shall perform their duties and responsibilities free from a prohibited conflict of interest, unless authorized by the Board or designee. Prohibited conflicts of interest include, but are not limited to:

1. soliciting or accepting anything of value (such as a gift, loan, contribution, or reward), other than compensation received from the District in exchange for services provided to the District, that would influence the employee's judgment when performing the employee's duties;
2. using public funds to purchase alcoholic beverages, jewelry, gifts, fees for golf, or any item the purchase or possession of which is illegal, except as consistent with and permitted by Policy 3205 and Revised School Code Section 1814;
3. using or authorizing the use of the employee's public employment or any confidential information received through public employment to obtain personal, professional, political, or financial gain other than compensation received from the District in exchange for services provided to the District for the employee or a member of the employee's immediate family, or a business with which the employee is associated;
4. using or authorizing the use of District personnel, resources, property, or funds under the employee's care and control other than in accordance with prescribed constitutional, statutory, and regulatory procedures, or using those items for personal, professional, political, or financial gain;
5. providing private services, lessons, tutoring, or coaching for students assigned to the employee for additional remuneration, except as permitted by Policy 4214;
6. engaging in any activity of a sexual or romantic nature with another employee(s) or contractor(s) that the employee supervises, unless the individuals are engaged to be married, married, or cohabitating;

7. engaging in any activity of a sexual or romantic nature on school property or at school-sponsored events;
8. directly or indirectly supervising, making, or contributing to an employment decision pertaining to a relative or significant other, or relative of a relative or significant other (as defined by Policy 4213);
9. engaging in any other activity that promotes an employee's financial and pecuniary interests over those of the District; and
10. entering into a proposed contract in which an administrator has a substantial conflict of interest (for Board members, see Policy 2301). Employees shall comply with the disclosure requirements in Policy 2301E(1).

C. Student Fraternization

Employees must establish and maintain professional boundaries with students, including while using personal or District technology. Employees are prohibited from direct or indirect interactions with students that do not reasonably relate to an educational purpose. Employees will behave at all times in a manner supportive of the best interests of students and the District.

Conduct identified below constitutes unprofessional conduct, subjecting the employee to discipline, including discharge, absent express Board or designee authorization. The following list illustrates prohibited behavior involving students but does not describe every kind of prohibited behavior:

1. communicating about alcohol use, drug use, or sexual activity when the discussion is not appropriately related to a specific aspect of the curriculum or the employee's duties;
2. providing drugs, alcohol, tobacco, e-cigarettes, or other items students cannot possess under the District's Student Code of Conduct;
3. commenting about matters involving sex, using double entendre, or making sexually suggestive remarks with no appropriate educational purpose;
4. displaying sexually inappropriate images, materials, or objects;
5. offering or soliciting sexual advice, whether written, verbal, or physical;
6. engaging in any activity of a sexual or romantic nature, including following graduation where the relationship arises out of an employee-student relationship;
7. inappropriate kissing;
8. inappropriately intruding on a student's personal space, such as by touching unnecessarily, moving too close, or staring at a portion of the student's body;

9. communicating directly or indirectly (e.g., by phone, email, text messaging, or social media) on a matter that does not pertain to school ~~unless the employee obtained prior parental consent~~ without first obtaining the express permission of the student's Parent ~~Parental and a District administrator~~. Electronic communications with students generally are to be sent simultaneously to multiple recipients and not just to one student except when the communication is clearly school related and inappropriate for persons other than the individual student to receive (e.g., grades);
10. permitting a specific student to engage in conduct that is not permitted or tolerated from other students;
11. inappropriately discussing with a student the student's personal issues or problems that should normally be discussed with a Parent or counselor unless the employee is the student's family member;
12. inappropriately giving a student a personal gift;
13. allowing a student to live in the employee's residence without first obtaining the express permission of the student's Parent ~~prior Parent consent~~ unless the student is the employee's family member, a foreign exchange student placed with the employee, or if the employee serves as the student's foster parent or legal guardian;
14. giving a student a ride in the employee's vehicle without appropriate authorization;
15. taking a student on an activity outside of school without first obtaining the express permission of the student's Parent and a District administrator;
16. inviting a student to the employee's home or residence without first obtaining the express permission of the student's Parent;
17. going to a student's home when the student's Parent or an adult chaperone is not present unless the employee is the student's family member; or
18. engaging in any other conduct which undermines the special position of trust and authority between a District employee and a student.

Formatted: Font color: Auto, Highlight

D. Abuse and Neglect

1. Children: An employee who suspects child abuse or neglect must: (a) immediately contact Children's Protective Services (CPS), (b) file an appropriate report with that agency as required by the Child Protection Law and Policy 4202, and (c) notify the Superintendent or designee and the building principal or supervisor that the report has been filed.

An employee should consult with their immediate supervisor about their duty to cooperate with CPS investigations or to disclose student records to CPS.

2. Vulnerable Adults: An employees who has reasonable cause to believe or suspect abuse, neglect, or exploitation of a vulnerable adult must: (a) immediately report the matter to Adult Protective Services (APS) consistent with Michigan's Social Welfare Act and Policy 4202 and (b) notify the Superintendent or designee and the building principal or supervisor that the report has been filed.

A reporter's identity will remain confidential unless disclosure is authorized by the reporter's consent or by court order.

An employee should consult with their immediate supervisor about their duty to cooperate with APS investigations or to disclose student records to APS.

Legal authority: MCL 380.11a, 380.601a, 380.634, 380.1308a, 380.1814; MCL 722.621 et seq.; MCL 400.11a.

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4205-AG-1 Criminal Justice Information Security (Non-Criminal Justice Agency)

The District will conduct background checks, consistent with Policy 4205(C) and Administrative Guideline 4205-AG-1, and will have the Michigan State Police ("MSP") obtain criminal history record information ("CHRI") from both the state and Federal Bureau of Investigation ("FBI") for all District employees, contractors, and vendors and their employees who regularly and continuously work under contract as provided in Policy 4205(C)(2). Employees who fail to follow these procedures will be subject to discipline subject to the Superintendent's review and written approval of any corrective action.

The District will provide employees, contractors, volunteers, and vendors and their employees for whom the District conducts background checks the most current version of the MSP RI-030 Live Scan consent form.

The District will complete and maintain a Noncriminal Justice Agency User Agreement (RI-087) provided by the Michigan State Police.

A. Local Agency Security Officer ("LASO")

The District Superintendent will appoint the Human Resources Generalist, a District employee, who: (1) is an authorized user, (2) has completed a fingerprint-based background check as required, (3) has been found appropriate to have access to CHRI, and (4) is directly involved in evaluating an individual's qualifications for employment or assignment as its LASO, who is responsible for the adoption of this guidance along with data/system security. When changes in the appointed LASO/CHRISS Administrator occur, the District will complete and return a new appointment notification form (CJIS-015) to MSP-CJIC-ATS@michigan.gov.

1. The LASO is responsible for ensuring:

- a. compliance with these regulations and laws;
- b. personnel security screening procedures are followed under this administrative guideline;
- c. approved and appropriate security measures are in place and functioning properly to protect CHRI;
- d. annual Awareness Training is being completed by all personnel authorized to access CHRI;
- e. only approved District employees have access to and are using the information in compliance with the law;
- f. compliance with this administrative guideline;

- g. that the MSP Information Security Officer (ISO) is promptly informed of any security incidents by submitted the MSP CJIS-016 Information Security Officer (ISO) Security Incident Report;
 - h. information security policy/procedures are reviewed and updated at least annually and after any security events involving CHRI; and
 - i. the District displays posters to increase security and privacy awareness of system users.
2. The LASO is also responsible for identifying and documenting, to the extent applicable:
 - a. District equipment connected to the MSP system; and
 - b. who is using or accessing CHRI and/or systems with access to CHRI.
 3. When a new LASO is established, the District will complete and deliver a LASO appointment form to the MSP and will keep a copy of the appointment form on file indefinitely. The LASO will make all MSP fingerprint account changes.

B. Personnel (Authorized User) Security

Only authorized users will have access to CHRI. An authorized user must be vetted through the national fingerprint background check and be given CHRI access by the LASO to evaluate potential employees, contractors, or volunteers for employment or assignment. If the District maintains digital CHRI, the LASO will assign authorized users unique passwords compliant to 4205-AG-1 (C)(3) to access it. Those who are not authorized users but who, by the function of their job, will be close to CHRI or computer systems with access to CHRI will be supervised by an authorized user. Employees who do not comply with state or federal laws or District policies or administrative guidelines will be subject to discipline, up to discharge.

1. Security with Separated Authorized Users

After an authorized user is separated from the District, that individual's access to CHRI will be terminated within 24 hours. This includes, but is not limited to, returning keys, access cards, and ceasing access to digital CHRI.

- a. The Human Resources director or designee must notify the LASO of the effective termination date of a user's employment by written email communication no later than 24 hours after the termination date.
- b. The Human Resources director or designee will require the return of any keys, access cards, files, and other related items.
- c. The LASO must ensure that access to the District's digital CHRI records system is disabled and the user's CHRIS account is deactivated.

2. Security with Transferred Authorized Users

When an authorized user is transferred or reassigned, the LASO will take steps necessary to block that individual's access to CHRI within 24 hours, unless the LASO determines that the individual must retain access.

C. Media Protection

Authorized users may only access CHRI on authorized devices, which does not include a personally owned mobile device, cell phone, computer, or other technology, consistent with specific terms and conditions, for access. All CHRI (including digital media) will be maintained in a physically secure location or controlled area. A physically secure location or controlled area will (1) be locked whenever an authorized user is not present or supervising and (2) limit access to unauthorized users. An authorized user accessing CHRI must position the media to prevent unauthorized users from accessing or viewing CHRI. Physical CHRI will be stored in a locked filing cabinet, safe, or vault. Digital CHRI will be encrypted consistent with FBI CJIS Security Policy. If digital CHRI is stored on a storage device without encryption, it must be stored like physical CHRI.

CJI and information system hardware, software and media are located and processed in the HR Offices at the Educational Services Center.

1. Media Transport

The LASO must approve all CHRI media transportation and will not grant approval unless transportation is reasonably justified. The LASO or LASO's designee will transport CHRI, which must be secured during transport. Physical CHRI must remain in the physical presence of authorized personnel until it is delivered. Physical CHRI must be transported in a sealed, locked, or secured medium and digital CHRI must be encrypted, and if not, secured in the same fashion as physical CHRI.

2. Media Disposal/Sanitization

CHRI media will be stored and retained for the duration required by law. Disposal must be made with the written approval of the LASO and the Superintendent. Only authorized users may dispose of CHRI media. Physical media will be cross-cut shredded or incinerated. Digital media must either be overwritten at least three (3) times or degaussed, passing a strong magnet over the media, before disposal or reuse. The LASO will keep written records (date and authorized user's signature) of CHRI media destroyed and the process for destroying or sanitizing CHRI media for ten (10) years.

3. Passwords

When the LASO assigns a unique password to an authorized user, it must have the following attributes:

- a. at least eight (8) characters;
- b. not consisting of only a proper noun or word found in a dictionary;
- c. not similar or identical to the username;
- d. not be displayed while entered or transmitted outside of the physically secure location or controlled area;
- e. expires every ninety (90) days; and
- f. cannot be the same as the previous ten (10) passwords.

4. Security Awareness and Incident Response Training and Testing

- a. The District will provide all authorized users role-based security and privacy and incident response training consistent with the following roles, as applicable:

Basic Role: users with unescorted access to a physically secure location;

General Role: users with physical and logical access to CJI;

Privileged Role: information technology personnel including system administrators, security administrators, network administrators and other similar roles;

Security Role: users responsible for ensuring confidentiality, integrity, and availability of CJI and compliant implementation of technology with the Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL).

- b. The District will provide users with security awareness training about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on handling information security incidents as follows:
 - i. for new users, prior to accessing CJI; and
 - ii. for all users annually about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on handling information security incidents;
 - iii. when required due to system changes; and
 - iv. within 30 days of any security event for individuals involved in the event.
- c. The LASO will keep a current record of all users who have completed training.

5. CHRI Dissemination

The District must maintain a record of any CHRI dissemination to another authorized agency for all dissemination outside the CHRIS system, consistent with the Revised School Code, which must include (1) date of release, (2) records released, (3) means of sharing, (4) District personnel who disseminated the CHRI, (5) whether authorization to disseminate was obtained, and (6) the agency to whom the CHRI was disseminated and (7) the recipient's name.

D. Incident Handling, Monitoring, and Reporting

1. In General

The District has established operational incident handling procedures for instances of an information security breach. The LASO will track CHRI security breach incidents and will report such incidents to the superintendent and MSP ISO using the MSP CJIS-016 reporting form. The District has provided specific incident handling capabilities for CHRI, consistent with the following table:

Capabilities shall be handled according to the following description:	Physical – Hard Copy CHRI	Digital – Digitally Accessed/Saved CHRI
Preparation	The CHRI container will be locked at all times in the office in which it is stored. When office staff is not present, the office must be locked.	Firewalls, anti-virus protection, and anti-malware/spyware protection will be maintained.
Detection	Physical intrusions to the building will be monitored. A Kent ISD ESC building alarm or video surveillance will monitor for physical or unauthorized intrusions. The building must be locked at night.	Electronic intrusions will be monitored by the virus and malware/spyware detection.
Analysis	The LASO will work with police authorities to determine how the incident occurred and what data was affected.	The IT department will determine what systems or data were affected and compromised.
Containment	The LASO will lock uncompromised CHRI in a secure container or transport CHRI to a secure area.	The IT department will stop the spread of any intrusion and prevent further damage.
Eradication	The LASO will work with local law enforcement [Kent County Sheriff /	The IT department will remove the intrusion

	Grand Rapids Township Police] to remove any threats that compromise CHRI data.	before restoring the system. All steps necessary to prevent recurrence will be taken before restoring the system.
Recovery	Local law enforcement [Kent County Sherriff / Grand Rapids Township Police] will handle and oversee the recovery of stolen CHRI media. The LASO may contact MSP for assistance in re-fingerprinting, if necessary.	The IT department will restore the agency information system and media to a safe environment.

2. CHRI Security Breach Incident

When a CHRI security breach incident occurs, the following will take place:

- a. Notice: Personnel will notify the LASO immediately or no later than one hour after the incident was discovered.
- b. Secure Systems: The LASO or appointed authorized user will stop any unauthorized access, secure the media, and shut down the systems necessary to avoid further unauthorized exposure.
- c. Assessment: The LASO will determine whether notification to individuals is needed, assess the extent of harm, and identify any applicable privacy requirements.
- d. Automated Reporting: Using automated mechanisms, such as email, website postings with automatic updates, and automated incident response tools, the LASO will report confirmed incidents to the CJIS Systems Officer (CSO), State Identification Bureaus Chief (SIB Chief), or Interface Agency Official.
- e. Supply Chain Coordination: The LASO will provide incident information to product or service providers or organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
- f. Records: The LASO or appointed authorized user will record all necessary information regarding the breach, the District's response to the breach, and who was involved in taking response measures.
- g. Coordination of Incident Handling and Contingency Planning: The LASO will coordinate incident handling activities with contingency planning activities and incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing implementing the resulting changes.

- h. Predictability: The LASO will ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
- i. Review of Policy/Procedures: The LASO will review and update information security policy/procedures at least annually and after security incidents involving CHRI.
- j. Legal Action: When such incident results in legal action (either civil or criminal) against a person or the District, the local law enforcement agency shall be contacted to collect, retain, and present evidence, according to the evidentiary rules of the appropriate jurisdiction(s).

E. Incident Response Support and Plan

1. Response Support Resource: The District will provide a response support resource that offers advice and assistance to system users for handling and reporting incidents.
2. Automation Support: The District will use automated mechanisms, such as access to a website or to an incident response vendor, to increase availability of incident response information and support.
3. Incident Response Plan: The District will develop an incident response plan that:
 - a. provides a roadmap for implementing incident response capability;
 - b. describes the structure and organization of incident response capability;
 - c. provides high-level approach for how incident response capability fits into overall organization;
 - d. meets unique requirements of the District related to mission, size, structure and functions;
 - e. defines reportable incidents;
 - f. provides metrics for measuring District incident response capability;
 - g. defines resources and management support needed to effectively maintain and mature an incident response capability;
 - h. addresses sharing of incident information;
 - i. is reviewed and approved by the superintendent annually; and
 - j. explicitly designates responsibility for incident response to District personnel with incident reporting responsibilities and CSO or CJIS WAN Official.

4. Incident Response Plan Management: The District will:
 - a. distribute the incident response plan to personnel with incident handling responsibilities;
 - b. update the incident response plan to address system and organizational changes or problems during plan implementation, execution or testing;
 - c. communicate incident response plan changes to District personnel with incident handling responsibilities; and
 - d. protect the incident response plan from unauthorized disclosure and modification.
5. Incident Response Plan Breaches: The District will include in the incident response plan for breaches involving personally identifiable information:
 - a. process to determine if notice to individuals or organization is needed;
 - b. assessment process to determine extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanism to mitigate such harms; and
 - c. identification of applicable privacy requirements.

F. Audit and Accountability

1. The District develops, documents, and disseminates to organizational personnel with audit and accountability responsibilities:
 - a. agency and system-level audit and accountability policy;
 - b. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance;
 - c. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 - d. procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.
2. The District reviews and updates the current audit and accountability policy and procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
3. The District identifies the types of events that the system is capable of logging in support of the audit function and coordinates the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.

4. The District specifies certain event types for logging within the system, provides rationale for the adequacy of the event types selected for logging, and annually reviews and updates the selected event types.
5. The District ensures that audit records contain information that establishes the following:
 - a. what type of event occurred;
 - b. when the event occurred;
 - c. where the event occurred;
 - d. source of the event;
 - e. outcome of the event; and
 - f. identity of any individuals, subjects, or objects/entities associated with the event.
6. The District generates audit records containing the following information:
 - a. session, connection, transaction, and activity duration;
 - b. source and destination addresses;
 - c. object or filename involved; and
 - d. number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
7. The District limits personally identifiable information contained in audit records to the minimum PII necessary to achieve the purpose for which it is collected.
8. The District allocates audit log storage capacity to accommodate the collection of audit logs to meet retention requirements.
9. The District alerts organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure and restarts all audit logging processes and verifies that systems are logging properly.
10. The District reviews and analyzes system audit records weekly and reports findings of potential or actual inappropriate or unusual activity to those with the relevant responsibilities.
11. The District adjusts the level of audit record review, analysis, and reporting within the system based on changes in input from law enforcement or intelligence agencies.

12. The District integrates audit record review, analysis, and reporting processes using automated mechanisms.
13. The District analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
14. The District provides and implements an audit record reduction and report generation capability that both supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations or incidents; and does not alter the original content or time ordering of audit records.

G. Access Control Policy

1. The District will develop, document, and disseminate to personnel with access control responsibilities:
 - a. Agency-level access control policy that:
 - i. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - ii. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
 - b. Procedures to facilitate implementation of the policy and the associated access controls.
2. The LASO will:
 - a. manage the development, documentation, and dissemination of the access control policy and procedures; and
 - b. review and update the access control policy annually and following any security breaches.

H. Account Management

1. The District will:
 - a. define and document the types of accounts allowed and specifically prohibited for use within the system;
 - b. prohibit use of personally-owned information systems, including mobile devices (i.e., bring your own device [BYOD]), and publicly accessible systems for accessing, processing, storing, or transmitting CJI;
 - c. assign account managers;
 - d. require conditions for group and role membership;

- e. specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and attributes listed for each account;
- f. at least annually, review accounts for compliance with account management requirements;
- g. establish and implement process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
- h. align account management processes with personnel termination and transfer processes.

I. Access Enforcement

The District will:

- 1. enforce approved authorization for logical access to information and system resources will be enforced in accordance with applicable access control policies; and
- 2. provide automated or manual processes to enable individuals to access elements of their personally identifiable information.

J. Information Flow Enforcement

The District will enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the District, and not passing any web requests to the public network that are not from the District-controlled or internal boundary protection devices.

K. Separation of Duties

The District will:

- 1. identify and document separation of duties based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI; and
- 2. define system access authorizations to support separation of duties.

L. Least Privilege

- 1. The District will allow only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
- 2. The District will:

- a. authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:
 - i. established system accounts, configured access authorizations, set events to be audited, set intrusion detection parameters, and other security functions; and
 - ii. security-relevant information in hardware, software, and firmware.
- b. require users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions;
- c. restrict privileged accounts on the system to privileged users;
- d. review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges;
- e. reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs; and
- f. log the execution of privileged functions.

M. Unsuccessful Logon Attempts

The District will enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minutes time period, and automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

N. System Use Notification (required when access via logon interfaces with human users)

1. A system use notification message will be displayed to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines stating that:
 - a. users are accessing a restricted information system;
 - b. system usage may be monitored, recorded, and subject to audit;
 - c. unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
 - d. use of the system indicates consent to monitoring and recording.

2. The notification message or banner will be retained on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access to the system.
3. For publicly accessible systems, before the District grants further access to publicly accessible systems:
 - a. system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines will be displayed;
 - b. references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities will be displayed; and.
 - c. a description of the authorized users of the system will be included.

O. Device Lock and Session Termination

1. The device lock will conceal information previously visible on the display with a publicly viewable image.
2. Further access to the system will be prevented by initiating a device lock after a maximum of 30 minutes of inactivity.
3. Users must log out when a work period has been completed.
4. Users must initiate a device lock before leaving the system unattended.
5. The device lock will be retained until the user reestablishes access using established identification and authentication procedures.

P. Remote Access

The District:

1. establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed;
2. authorizes each type of remote access to the system prior to allowing such connections;
3. employs automated mechanisms to monitor and control remote access methods;
4. implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions;
5. routes remote access through authorized and managed network access control points;

6. authorizes the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs; and
7. documents the rationale for remote access in the security plan for the system.

Q. Wireless Access

The District:

1. establishes configuration requirements, connection requirements, and implementation guidance for each type of wireless access;
2. authorizes each type of wireless access to the system prior to allowing such connections;
3. protects wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption; and
4. disables wireless networking capabilities embedded within system components prior to issuance and deployment when not intended for use.

R. Access Control for Mobile Devices

The District:

1. establishes configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas;
2. authorizes the connection of mobile devices to organizational systems; and
3. employs full-device encryption to protect the confidentiality and integrity of information on full-and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.

S. Use of External Systems

1. The District permits authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
 - a. verification of implementation of controls on external system as specified in the District's security and privacy policies and security and privacy plans; or
 - b. retention of approved system connection or processing agreements with the organizational entity hosting the external system.

2. The District restricts the use of District-controlled portable storage devices in external systems including how the devices may be used and under what conditions the devices may be used.

T. Information Sharing

The District:

1. enables authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and
2. employs attribute-based access control or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.

U. Identification and Authentication (IA) (CJISSECPOL 5.6)

V. Physical and Environmental Protection (CJISSECPOL 5.9)

W. Systems and Communications Protection (CJISSECPOL 5.10)

X. System and Services Acquisition (CJISSECPOL 5.14)

Y. System and Information Integrity (CJISSECPOL 5.15)

Z. Maintenance (CJISSECPOL 5.16)

AA. Planning (CJISSECPOL 5.17)

BB. Contingency Planning (CJISSECPOL 5.18)

CC. Risk Assessment (CJISSECPOL 5.19)

**Legal authority: Criminal Justice Information Services (CJIS) Security Policy 6.0
December 27, 2024**

Date adopted: August 19, 2024

Date revised: July 20, 2026

Series 4000: District Employment

4200 Employee Conduct and Ethics

4205-AG-1 Criminal Justice Information Security (Non-Criminal Justice Agency)

The District will conduct background checks, consistent with Policy 4205(C) and Administrative Guideline 4205-AG-1, and will have the Michigan State Police ("MSP") obtain criminal history record information ("CHRI") from both the state and Federal Bureau of Investigation ("FBI") for all District employees, contractors, and vendors and their employees who regularly and continuously work under contract as provided in Policy 4205(C)(2). Employees who fail to follow these procedures will be subject to discipline subject to the Superintendent's review and written approval of any corrective action.

The District will provide employees, contractors, volunteers, and vendors and their employees for whom the District conducts background checks the most current version of the MSP RI-030 Live Scan consent form.

The District will complete and maintain a Noncriminal Justice Agency User Agreement (RI-087) provided by the Michigan State Police.

A. Local Agency Security Officer ("LASO")

The District Superintendent will appoint the [REDACTED] [Note: add the position of individual. Delete this note upon designation], a District employee, who: (1) is an authorized user, (2) has completed a fingerprint-based background check as required, (3) has been found appropriate to have access to CHRI, and (4) is directly involved in evaluating an individual's qualifications for employment or assignment as its LASO, who is responsible for the adoption of this guidance along with data/system security. When changes in the appointed LASO/CHRISS Administrator occur, the District will complete and return a new appointment notification form (CJIS-015) to MSP-CJIC-ATS@michigan.gov.

1. The LASO is responsible for ensuring:
 - a. compliance with these regulations and laws;
 - b. personnel security screening procedures are followed under this administrative guideline;
 - c. approved and appropriate security measures are in place and functioning properly to protect CHRI;
 - d. annual Awareness Training is being completed by all personnel authorized to access CHRI;
 - e. only approved District employees have access to and are using the information in compliance with the law;
 - f. compliance with this administrative guideline;

- g. that the MSP Information Security Officer (ISO) is promptly informed of any security incidents by submitted the MSP CJIS-016 Information Security Officer (ISO) Security Incident Report;
 - h. information security policy/procedures are reviewed and updated at least annually and after any security events involving CHRI; and
 - i. the District [Note: Select one or more. Delete this note and retain at least one listed item: (1) displays posters, (2) offers supplies inscribed with security and privacy reminders, (3) displays logon screen messages, (4) generates email advisories or notices from District officials, or (5) conducts awareness events] to increase security and privacy awareness of system users.
2. The LASO is also responsible for identifying and documenting, to the extent applicable:
 - a. District equipment connected to the MSP system; and
 - b. who is using or accessing CHRI and/or systems with access to CHRI.
 3. When a new LASO is established, the District will complete and deliver a LASO appointment form to the MSP and will keep a copy of the appointment form on file indefinitely. The LASO will make all MSP fingerprint account changes.

B. Personnel (Authorized User) Security

Only authorized users will have access to CHRI. An authorized user must be vetted through the national fingerprint background check and be given CHRI access by the LASO to evaluate potential employees, contractors, or volunteers for employment or assignment. If the District maintains digital CHRI, the LASO will assign authorized users unique passwords compliant to 4205-AG-1 (C)(3) to access it. Those who are not authorized users but who, by the function of their job, will be close to CHRI or computer systems with access to CHRI will be supervised by an authorized user. Employees who do not comply with state or federal laws or District policies or administrative guidelines will be subject to discipline, up to discharge.

1. Security with Separated Authorized Users

After an authorized user is separated from the District, that individual's access to CHRI will be terminated within 24 hours. This includes, but is not limited to, returning keys, access cards, and ceasing access to digital CHRI.

- a. The Human Resources director or designee must notify the LASO of the effective termination date of a user's employment by written email communication no later than 24 hours after the termination date.
- b. The Human Resources director or designee will require the return of any keys, access cards, files, and other related items.



- c. The LASO must ensure that access to the District's digital CHRI records system is disabled and the user's CHRISS account is deactivated.

2. Security with Transferred Authorized Users

When an authorized user is transferred or reassigned, the LASO will take steps necessary to block that individual's access to CHRI within 24 hours, unless the LASO determines that the individual must retain access.

C. Media Protection

Authorized users may only access CHRI on authorized devices, which does not include a personally owned mobile device, cell phone, computer, or other technology, consistent with specific terms and conditions, for access. All CHRI (including digital media) will be maintained in a physically secure location or controlled area. A physically secure location or controlled area will (1) be locked whenever an authorized user is not present or supervising and (2) limit access to unauthorized users. An authorized user accessing CHRI must position the media to prevent unauthorized users from accessing or viewing CHRI. Physical CHRI will be stored in a locked filing cabinet, safe, or vault. Digital CHRI will be encrypted consistent with FBI CJIS Security Policy. If digital CHRI is stored on a storage device without encryption, it must be stored like physical CHRI.

CJI and information system hardware, software and media are located and processed in [add: location and description].

1. Media Transport

The LASO must approve all CHRI media transportation and will not grant approval unless transportation is reasonably justified. The LASO or LASO's designee will transport CHRI, which must be secured during transport. Physical CHRI must remain in the physical presence of authorized personnel until it is delivered. Physical CHRI must be transported in a sealed, locked, or secured medium and digital CHRI must be encrypted, and if not, secured in the same fashion as physical CHRI.

2. Media Disposal/Sanitization

CHRI media will be stored and retained for the duration required by law. Disposal must be made with the written approval of the LASO and the Superintendent. Only authorized users may dispose of CHRI media. Physical media will be cross-cut shredded or incinerated. Digital media must either be overwritten at least three (3) times or degaussed, passing a strong magnet over the media, before disposal or reuse. The LASO will keep written records (date and authorized user's signature) of CHRI media destroyed and the process for destroying or sanitizing CHRI media for ten (10) years.

3. Passwords

When the LASO assigns a unique password to an authorized user, it must have the following attributes:

- a. at least eight (8) characters;
- b. not consisting of only a proper noun or word found in a dictionary;
- c. not similar or identical to the username;
- d. not be displayed while entered or transmitted outside of the physically secure location or controlled area;
- e. expires every ninety (90) days; and
- f. cannot be the same as the previous ten (10) passwords.

4. Security Awareness and Incident Response Training and Testing

- a. The District will provide all authorized users role-based security and privacy and incident response training consistent with the following roles, as applicable:

Basic Role: users with unescorted access to a physically secure location;

General Role: users with physical and logical access to CJI;

Privileged Role: information technology personnel including system administrators, security administrators, network administrators and other similar roles;

Security Role: users responsible for ensuring confidentiality, integrity, and availability of CJI and compliant implementation of technology with the Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL).

- b. The District will provide users with security awareness training about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on handling information security incidents as follows:
 - i. for new users, prior to accessing CJI; and
 - ii. for all users annually about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on handling information security incidents;
 - iii. when required due to system changes; and
 - iv. within 30 days of any security event for individuals involved in the event.

- c. The LASO will keep a current record of all users who have completed training.

5. CHRI Dissemination

The District must maintain a record of any CHRI dissemination to another authorized agency for all dissemination outside the CHRIS system, consistent with the Revised School Code, which must include (1) date of release, (2) records released, (3) means of sharing, (4) District personnel who disseminated the CHRI, (5) whether authorization to disseminate was obtained, and (6) the agency to whom the CHRI was disseminated and (7) the recipient's name.

D. Incident Handling, Monitoring, and Reporting

1. In General

The District has established operational incident handling procedures for instances of an information security breach. The LASO will track CHRI security breach incidents and will report such incidents to the superintendent and MSP ISO using the MSP CJIS-016 reporting form. The District has provided specific incident handling capabilities for CHRI, consistent with the following table:

Capabilities shall be handled according to the following description:	Physical – Hard Copy CHRI	Digital – Digitally Accessed/Saved CHRI
Preparation	The CHRI container will be locked at all times in the office in which it is stored. When office staff is not present, the office must be locked.	Firewalls, anti-virus protection, and anti-malware/spyware protection will be maintained.
Detection	Physical intrusions to the building will be monitored. A [add company name of building alarm] building alarm or video surveillance will monitor for physical or unauthorized intrusions. The building must be locked at night.	Electronic intrusions will be monitored by the virus and malware/spyware detection.
Analysis	The LASO will work with police authorities to determine how the incident occurred and what data was affected.	The IT department will determine what systems or data were affected and compromised.

Containment	The LASO will lock uncompromised CHRI in a secure container or transport CHRI to a secure area.	The IT department will stop the spread of any intrusion and prevent further damage.
Eradication	The LASO will work with local law enforcement [name police department] to remove any threats that compromise CHRI data.	The IT department will remove the intrusion before restoring the system. All steps necessary to prevent recurrence will be taken before restoring the system.
Recovery	Local law enforcement [name police department] will handle and oversee the recovery of stolen CHRI media. The LASO may contact MSP for assistance in re-fingerprinting, if necessary.	The IT department will restore the agency information system and media to a safe environment.

2. CHRI Security Breach Incident

When a CHRI security breach incident occurs, the following will take place:

- a. Notice: Personnel will notify the LASO immediately or no later than one hour after the incident was discovered.
- b. Secure Systems: The LASO or appointed authorized user will stop any unauthorized access, secure the media, and shut down the systems necessary to avoid further unauthorized exposure.
- c. Assessment: The LASO will determine whether notification to individuals is needed, assess the extent of harm, and identify any applicable privacy requirements.
- d. Automated Reporting: Using automated mechanisms, such as email, website postings with automatic updates, and automated incident response tools, the LASO will report confirmed incidents to the CJIS Systems Officer (CSO), State Identification Bureaus Chief (SIB Chief), or Interface Agency Official.
- e. Supply Chain Coordination: The LASO will provide incident information to product or service providers or organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
- f. Records: The LASO or appointed authorized user will record all necessary information regarding the breach, the District's response to the breach, and who was involved in taking response measures.

- g. Coordination of Incident Handling and Contingency Planning: The LASO will coordinate incident handling activities with contingency planning activities and incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing implementing the resulting changes.
- h. Predictability: The LASO will ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
- i. Review of Policy/Procedures: The LASO will review and update information security policy/procedures at least annually and after security incidents involving CHRI.
- j. Legal Action: When such incident results in legal action (either civil or criminal) against a person or the District, the local law enforcement agency shall be contacted to collect, retain, and present evidence, according to the evidentiary rules of the appropriate jurisdiction(s).

E. Incident Response Support and Plan

- 1. Response Support Resource: The District will provide a response support resource that offers advice and assistance to system users for handling and reporting incidents.
- 2. Automation Support: The District will use automated mechanisms, such as access to a website or to an incident response vendor, to increase availability of incident response information and support.
- 3. Incident Response Plan: The District will develop an incident response plan that:
 - a. provides a roadmap for implementing incident response capability;
 - b. describes the structure and organization of incident response capability;
 - c. provides high-level approach for how incident response capability fits into overall organization;
 - d. meets unique requirements of the District related to mission, size, structure and functions;
 - e. defines reportable incidents;
 - f. provides metrics for measuring District incident response capability;
 - g. defines resources and management support needed to effectively maintain and mature an incident response capability;
 - h. addresses sharing of incident information;



- i. is reviewed and approved by the superintendent annually; and
 - j. explicitly designates responsibility for incident response to District personnel with incident reporting responsibilities and CSO or CJIS WAN Official.
4. Incident Response Plan Management: The District will:
- a. distribute the incident response plan to personnel with incident handling responsibilities;
 - b. update the incident response plan to address system and organizational changes or problems during plan implementation, execution or testing;
 - c. communicate incident response plan changes to District personnel with incident handling responsibilities; and
 - d. protect the incident response plan from unauthorized disclosure and modification.
5. Incident Response Plan Breaches: The District will include in the incident response plan for breaches involving personally identifiable information:
- a. process to determine if notice to individuals or organization is needed;
 - b. assessment process to determine extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanism to mitigate such harms; and
 - c. identification of applicable privacy requirements.

F. Audit and Accountability

1. The District develops, documents, and disseminates to organizational personnel with audit and accountability responsibilities:
 - a. agency and system-level audit and accountability policy;
 - b. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance;
 - c. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 - d. procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.
2. The District reviews and updates the current audit and accountability policy and procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

3. The District identifies the types of events that the system is capable of logging in support of the audit function and coordinates the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.
4. The District specifies certain event types for logging within the system, provides rationale for the adequacy of the event types selected for logging, and annually reviews and updates the selected event types.
5. The District ensures that audit records contain information that establishes the following:
 - a. what type of event occurred;
 - b. when the event occurred;
 - c. where the event occurred;
 - d. source of the event;
 - e. outcome of the event; and
 - f. identity of any individuals, subjects, or objects/entities associated with the event.
6. The District generates audit records containing the following information:
 - a. session, connection, transaction, and activity duration;
 - b. source and destination addresses;
 - c. object or filename involved; and
 - d. number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
7. The District limits personally identifiable information contained in audit records to the minimum PII necessary to achieve the purpose for which it is collected.
8. The District allocates audit log storage capacity to accommodate the collection of audit logs to meet retention requirements.
9. The District alerts organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure and restarts all audit logging processes and verifies that systems are logging properly.
10. The District reviews and analyzes system audit records weekly and reports findings of potential or actual inappropriate or unusual activity to those with the relevant responsibilities.

11. The District adjusts the level of audit record review, analysis, and reporting within the system based on changes in input from law enforcement or intelligence agencies.
12. The District integrates audit record review, analysis, and reporting processes using automated mechanisms.
13. The District analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
14. The District provides and implements an audit record reduction and report generation capability that both supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations or incidents; and does not alter the original content or time ordering of audit records.

G. Access Control Policy

1. The District will develop, document, and disseminate to personnel with access control responsibilities:
 - a. Agency-level access control policy that:
 - i. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - ii. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
 - b. Procedures to facilitate implementation of the policy and the associated access controls.
2. The LASO will:
 - a. manage the development, documentation, and dissemination of the access control policy and procedures; and
 - b. review and update the access control policy annually and following any security breaches.

H. Account Management

1. The District will:
 - a. define and document the types of accounts allowed and specifically prohibited for use within the system;
 - b. prohibit use of personally-owned information systems, including mobile devices (i.e., bring your own device [BYOD]), and publicly accessible systems for accessing, processing, storing, or transmitting CJI;

- c. assign account managers;
- d. require conditions for group and role membership;
- e. specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and attributes listed for each account;
- f. at least annually, review accounts for compliance with account management requirements;
- g. establish and implement process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
- h. align account management processes with personnel termination and transfer processes.

I. Access Enforcement

The District will:

- 1. enforce approved authorization for logical access to information and system resources will be enforced in accordance with applicable access control policies; and
- 2. provide automated or manual processes to enable individuals to access elements of their personally identifiable information.

J. Information Flow Enforcement

The District will enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the District, and not passing any web requests to the public network that are not from the District-controlled or internal boundary protection devices.

K. Separation of Duties

The District will:

- 1. identify and document separation of duties based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI; and
- 2. define system access authorizations to support separation of duties.

L. Least Privilege

- 1. The District will allow only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

2. The District will:

- a. authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:
 - i. established system accounts, configured access authorizations, set events to be audited, set intrusion detection parameters, and other security functions; and
 - ii. security-relevant information in hardware, software, and firmware.
- b. require users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions;
- c. restrict privileged accounts on the system to privileged users;
- d. review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges;
- e. reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs; and
- f. log the execution of privileged functions.

M. Unsuccessful Logon Attempts

The District will enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minutes time period, and automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

N. System Use Notification (required when access via logon interfaces with human users)

1. A system use notification message will be displayed to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines stating that:
 - a. users are accessing a restricted information system;
 - b. system usage may be monitored, recorded, and subject to audit;
 - c. unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
 - d. use of the system indicates consent to monitoring and recording.

2. The notification message or banner will be retained on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access to the system.
3. For publicly accessible systems, before the District grants further access to publicly accessible systems:
 - a. system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines will be displayed;
 - b. references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities will be displayed; and.
 - c. a description of the authorized users of the system will be included.

O. Device Lock and Session Termination

1. The device lock will conceal information previously visible on the display with a publicly viewable image.
2. Further access to the system will be prevented by initiating a device lock after a maximum of 30 minutes of inactivity.
3. Users must log out when a work period has been completed.
4. Users must initiate a device lock before leaving the system unattended.
5. The device lock will be retained until the user reestablishes access using established identification and authentication procedures.

P. Remote Access

The District:

1. establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed;
2. authorizes each type of remote access to the system prior to allowing such connections;
3. employs automated mechanisms to monitor and control remote access methods;
4. implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions;
5. routes remote access through authorized and managed network access control points;

6. authorizes the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs; and
7. documents the rationale for remote access in the security plan for the system.

Q. Wireless Access

The District:

1. establishes configuration requirements, connection requirements, and implementation guidance for each type of wireless access;
2. authorizes each type of wireless access to the system prior to allowing such connections;
3. protects wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption; and
4. disables wireless networking capabilities embedded within system components prior to issuance and deployment when not intended for use.

R. Access Control for Mobile Devices

The District:

1. establishes configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas;
2. authorizes the connection of mobile devices to organizational systems; and
3. employs full-device encryption to protect the confidentiality and integrity of information on full-and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.

S. Use of External Systems

1. The District permits authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
 - a. verification of implementation of controls on external system as specified in the District's security and privacy policies and security and privacy plans; or
 - b. retention of approved system connection or processing agreements with the organizational entity hosting the external system.

2. The District restricts the use of District-controlled portable storage devices in external systems including how the devices may be used and under what conditions the devices may be used.

T. Information Sharing

The District:

1. enables authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and
2. employs attribute-based access control or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.

U. Identification and Authentication (IA) (CJISSECPOL 5.6)

V. Physical and Environmental Protection (CJISSECPOL 5.9)

W. Systems and Communications Protection (CJISSECPOL 5.10)

X. System and Services Acquisition (CJISSECPOL 5.14)

Y. System and Information Integrity (CJISSECPOL 5.15)

Z. Maintenance (CJISSECPOL 5.16)

AA. Planning (CJISSECPOL 5.17)

BB. Contingency Planning (CJISSECPOL 5.18)

CC. Risk Assessment (CJISSECPOL 5.19)

Legal authority: Criminal Justice Information Services (CJIS) Security Policy 6.0
December 27, 2024

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4209 Abortion Referrals and Assistance

A District official, Board member, or District employee shall not refer a student for an abortion or assist a student with obtaining an abortion. This prohibition does not apply to a person who is the Parent of that student.

Legal Authority: MCL 380.11a

Date Adopted: August 15, 2022

Date Revised: August 19, 2024

Date Revised: July 20, 2026

Series 4000: District Employment

4200 Employee Conduct and Ethics

4209 *Abortion Referrals and Assistance* [Optional] [Note: If the Board elects not to adopt this Policy, delete the body of the policy and replace the title with "Intentionally Left Blank" after the policy number and in the Table of Contents to ensure accurate numbering of subsequent policies in the Policy Manual.]

A District official, Board member, or District employee shall not refer a student for an abortion or assist a student with obtaining an abortion. This prohibition does not apply to a person who is the Parent of that student.

Legal Authority: MCL 380.11a~~s~~

Date Adopted:

Date Revised:



Series 4000: District Employment

4200 Employee Conduct and Ethics

4210 *Drug and Alcohol Free Workplace; Tobacco Product Restrictions*

A. General

Employees serve as role models to students at school and in the community. Employee substance abuse constitutes a threat to the physical and mental well-being of employees and students and significantly impedes job performance and effectiveness.

The District maintains a drug and alcohol free workplace. In addition, to the extent permitted by law, the District strives to maintain a tobacco product free workplace.

This policy does not prohibit the use of nicotine replacement therapies for smoking cessation, such as Food and Drug Administration approved nicotine gum, patches, or lozenges.

B. Definitions

1. "District premises" means District buildings, facilities, or other District property which is owned, leased, or used for a District purpose or District-owned vehicles or vehicles used for a District purpose.
2. "District purpose or function" means a District-sponsored or District-approved activity, event, function or other activity performed by an employee under the District's jurisdiction, which is within the scope of employment, duties, or job description.
3. "Electronic nicotine delivery system" means any product containing or delivering nicotine, a nicotine analog, or any other substance, whether natural or synthetic, intended for human consumption through the inhalation of aerosol or vapor from the product. "Electronic nicotine delivery system" includes, but is not limited to, devices manufactured, marketed, or sold as e-cigarettes, e-cigars, e-pipes, e-hookah, vape pens, mods, and tank systems, regardless of any other product name or descriptor that is used. "Electronic nicotine delivery system" includes any component part of a product, whether marketed or sold separately, including but not limited to e-liquids, e-juice, cartridges, and pods.
4. "Illicit substance" means any consumable alcohol; illegal drugs, including but not limited to those substances defined as "controlled substances" pursuant to federal or state law; marihuana; anabolic steroids, human growth hormones or other performance-enhancing drugs; and substances purported to be illegal, abusive, or performance-enhancing (i.e., "look-alike" drugs). This definition also includes any other substance used by an employee as an intoxicant.

5. "Imitation tobacco product" means any edible non-tobacco product designed to resemble a commercial tobacco product, or any non-edible non-tobacco product designed to resemble a commercial tobacco product and intended to be used by children as a toy. "Imitation tobacco product" includes, but is not limited to, candy or chocolate cigarettes, bubble gum cigars, shredded bubble gum resembling chewing tobacco, pouches containing flavored substances packaged similar to snus, and shredded beef jerky in containers resembling snuff tins.
6. "Reasonable suspicion" means specific, contemporaneous, and articulable observations concerning an employee's behavior, speech, appearance, or odor that suggests the employee is under the influence of an illicit substance.
7. "Smoking" means inhaling, exhaling, burning, or carrying any lighted or heated cigar, cigarette, or pipe, or any other lighted or heated product containing, made, or derived from nicotine, tobacco, cannabis, or other plant, whether natural or synthetic, that is intended for inhalation. "Smoking" also includes carrying or using an activated electronic nicotine delivery system. "Smoking" does not include the use of traditional or sacred tobacco used by many Native communities for spiritual and medicinal purposes.
8. "Tobacco industry" means manufacturers, distributors, or wholesalers of tobacco products or tobacco-related devices (e.g., Juul, Altria). This includes parent companies and subsidiaries.
9. "Tobacco product or commercial tobacco product" means any product containing, made, or derived from tobacco or that contains nicotine, whether synthetic or natural, that is intended for human consumption, whether chewed, smoked, absorbed, dissolved, inhaled, snorted, sniffed, or ingested by any other means, or any component, part, or accessory of a tobacco product, including but not limited to: cigarettes; electronic nicotine delivery systems; cigars; little cigars; cheroots; stogies; periques; granulated, plug cut, crimp cut, ready rubbed, and other smoking tobacco; snuff; snuff flour; cavendish; plug and twist tobacco; fine-cut and other chewing tobacco; shorts; refuse scraps, clippings, cuttings and sweepings of tobacco; and other kinds and forms of tobacco.
10. "Tobacco-related device" means ashtrays, rolling papers, wraps, or pipes for smoking and any components, parts, or accessories of electronic nicotine delivery systems.
11. "Under the influence" means the use or misuse of an illicit substance or other intoxicant (including over-the-counter and prescription medication) by an employee that in any degree impairs, negatively affects, or tends to deprive that person of any physical or mental capacity normally possessed and required to perform job responsibilities.
12. "Use of tobacco product" means any of the following:

- a. the carrying by a person of a lighted cigar, cigarette, pipe, other lighted smoking device, or electronic nicotine delivery system;
- b. the inhaling or chewing of a tobacco product;
- c. the placing of a tobacco product within a person's mouth; or
- d. the smoking or use of an electronic nicotine delivery system, imitation tobacco product, or other substitute forms of cigarettes, clove cigarettes, or other lighted smoking devices for consuming or inhaling tobacco, nicotine, or any other substance.

C. Standards of Conduct

Employees are prohibited from the following conduct on District premises, at a District function:

1. manufacturing, selling, soliciting, possessing, using (including application, injection, inhalation, or ingestion), dispensing, or distributing any illicit substance;
2. being under the influence as defined in this Policy;
3. misusing over-the-counter and prescription medications;
4. manufacturing, selling, soliciting, dispensing, displaying, promoting, or distributing any tobacco product, tobacco-related device, or imitation tobacco product. This includes products or paraphernalia displaying tobacco industry brand; or
5. using or consuming a tobacco product on District premises or at a District function.

Violating these standards will subject an employee to discipline, including discharge.

It shall be a violation of this Policy for an employee to solicit or accept any contributions, gifts, money, curricula, or materials from the tobacco industry or from any tobacco products shop for use at a District premises or District function. This includes, but is not limited to, donations, money for sponsorship, advertising material, alleged educational materials, promotions, loans, scholarships, or support for equipment, uniforms, sports, or training facilities. It shall also be a violation of this Policy to participate in any type of service funded by the tobacco industry on District premises or at a District function.

If a reasonable suspicion exists that an employee is under the influence, the Superintendent or designee may direct the employee to submit to a drug test or breathalyzer. If the employee refuses, the employee may be subject to discipline, including discharge, based on the District's observations.

D. It shall not be a violation of this policy:

1. for commercial tobacco products, tobacco-related devices, imitation tobacco products, or lighters to be included in an instructional or work-related activity in the District school buildings if the activity is conducted by a staff member or an approved visitor and the activity does not include smoking, chewing, or otherwise ingesting the product;
2. for a person to possess or provide tobacco, tobacco-related devices, imitation tobacco products, or lighters to any other person as part of an indigenous practice used by Native communities for spiritual and medicinal purposes. It shall not be a violation of this policy to use tobacco, tobacco-related devices, initiation tobacco products, or lighters as part of an educational experience related to traditional or sacred tobacco practices that has been approved by administrators;
3. to use or possess a product that has been approved by the U.S. Food and Drug Administration for sale as a tobacco cessation product, as a nicotine dependence product, or for other medical purposes, and is being marketed and sold solely for such an approved purpose.

E. Support

Administrators shall consult with the local public health department or other appropriate health and allied community-based organizations to provide students, staff, and administrators with information and access to support systems, programs, and services to encourage them to abstain from the use of commercial tobacco products. Administrators shall identify and offer evidence-based programs and services for individuals that use commercial tobacco products to support them in complying with this policy.

F. Notice

The District shall provide notice of this policy in staff handbooks, through orientations and employee or staff training, and when offering employment.

Legal authority: 20 USC 7101 et seq.; 41 USC 8101 et seq.; 42 USC 12101 et seq.; Schedules I-V of Chapter 13 of the Controlled Substances Act, 21 USC 812; 29 USC 701 et seq.; MCL 37.1211; Schedules 1-5 of the Michigan Uniform Controlled Substances Act, MCL 333.7201 et seq.; MCL 380.11a, 380.601a; MCL 436.1101 et seq.; MCL 750.473.

Date adopted: August 15, 2022

Date revised: July 20, 2026

Series 4000: District Employment

4200 Employee Conduct and Ethics

4210 Drug and Alcohol Free Workplace; Tobacco Product Restrictions

A. General

Employees serve as role models to students at school and in the community. Employee substance abuse constitutes a threat to the physical and mental well-being of employees and students and significantly impedes job performance and effectiveness.

The District maintains a drug and alcohol free workplace. In addition, to the extent permitted by law, the District strives to maintain a tobacco product free workplace.

This policy does not prohibit the use of nicotine replacement therapies for smoking cessation, such as Food and Drug Administration approved nicotine gum, patches, or lozenges.

B. Definitions

1. "District premises" means District buildings, facilities, or other District property which is owned, leased, or used for a District purpose or District-owned vehicles or vehicles used for a District purpose.
2. "District purpose or function" means a District-sponsored or District-approved activity, event, function or other activity performed by an employee under the District's jurisdiction, which is within the scope of employment, duties, or job description.
3. "Electronic nicotine delivery system" means any product containing or delivering nicotine, a nicotine analog, or any other substance, whether natural or synthetic, intended for human consumption through the inhalation of aerosol or vapor from the product. "Electronic nicotine delivery system" includes, but is not limited to, devices manufactured, marketed, or sold as e-cigarettes, e-cigars, e-pipes, e-hookah, vape pens, mods, and tank systems, regardless of any other product name or descriptor that is used. "Electronic nicotine delivery system" includes any component part of a product, whether marketed or sold separately, including but not limited to e-liquids, e-juice, cartridges, and pods.
4. "Illicit substance" means any consumable alcohol; illegal drugs, including but not limited to those substances defined as "controlled substances" pursuant to federal or state law; marihuana; anabolic steroids, human growth hormones or other performance-enhancing drugs; and substances purported to be illegal, abusive, or performance-enhancing (i.e., "look-alike" drugs). This definition also includes any other substance used by an employee as an intoxicant.

5. "Imitation tobacco product" means any edible non-tobacco product designed to resemble a commercial tobacco product, or any non-edible non-tobacco product designed to resemble a commercial tobacco product and intended to be used by children as a toy. "Imitation tobacco product" includes, but is not limited to, candy or chocolate cigarettes, bubble gum cigars, shredded bubble gum resembling chewing tobacco, pouches containing flavored substances packaged similar to snus, and shredded beef jerky in containers resembling snuff tins.
6. "Reasonable suspicion" means specific, contemporaneous, and articulable observations concerning an employee's behavior, speech, appearance, ~~or~~ odor that suggests the employee is under the influence of an illicit substance.
7. "Smoking" means inhaling, exhaling, burning, or carrying any lighted or heated cigar, cigarette, or pipe, or any other lighted or heated product containing, made, or derived from nicotine, tobacco, cannabis, or other plant, whether natural or synthetic, that is intended for inhalation. "Smoking" also includes carrying or using an activated electronic nicotine delivery system. "Smoking" does not include the use of traditional or sacred tobacco used by many Native communities for spiritual and medicinal purposes.
8. "Tobacco industry" means manufacturers, distributors, or wholesalers of tobacco products or tobacco-related devices (e.g., Juul, Altria). This includes parent companies and subsidiaries.
9. "Tobacco product or commercial tobacco product" means any product containing, made, or derived from tobacco or that contains nicotine, whether synthetic or natural, that is intended for human consumption, whether chewed, smoked, absorbed, dissolved, inhaled, snorted, sniffed, or ingested by any other means, or any component, part, or accessory of a tobacco product, including but not limited to: cigarettes; electronic nicotine delivery systems; cigars; little cigars; cheroots; stogies; periques; granulated, plug cut, crimp cut, ready rubbed, and other smoking tobacco; snuff; snuff flour; cavendish; plug and twist tobacco; fine-cut and other chewing tobacco; shorts; refuse scraps, clippings, cuttings and sweepings of tobacco; and other kinds and forms of tobacco.
10. "Tobacco-related device" means ashtrays, rolling papers, wraps, or pipes for smoking and any components, parts, or accessories of electronic nicotine delivery systems.
- ~~2.1. "District premises" means District buildings, facilities, or other District property which is owned, leased, or used for a District purpose or District-owned vehicles or vehicles used for a District purpose.~~
- ~~3.1. "District purpose or function" means a District-sponsored or District-approved activity, event, function or other activity performed by an employee~~

~~under the District's jurisdiction, which is within the scope of employment, duties, or job description.~~

4. ~~"Tobacco product" means a form of tobacco intended to be inhaled, chewed, or placed in a person's mouth.~~

5.11. "Under the influence" means the use or misuse of an illicit substance or other intoxicant (including over-the-counter and prescription medication) by an employee that in any degree impairs, negatively affects, or tends to deprive that person of any physical or mental capacity normally possessed and required to perform job responsibilities.

12. "Use of tobacco product" means any of the following:

- a. the carrying by a person of a lighted cigar, cigarette, pipe, other lighted smoking device, or electronic nicotine delivery system;
- b. the inhaling or chewing of a tobacco product;
- c. the placing of a tobacco product within a person's mouth; or
- d. the smoking or use of an electronic nicotine delivery system, imitation tobacco product, or other substitute forms of cigarettes, clove cigarettes, or other lighted smoking devices for consuming or inhaling tobacco, nicotine, or any other substance.

C. Standards of Conduct

Employees are prohibited from the following conduct on District premises ~~or~~ at a District function:

- 1. manufacturing, selling, soliciting, possessing, using (including application, injection, inhalation, or ingestion), dispensing, or distributing any illicit substance;
- 2. being under the influence as defined in this Policy;
- 3. misusing over-the-counter and prescription medications;
- 4. manufacturing, selling, soliciting, dispensing, displaying, promoting, or distributing any tobacco product, tobacco-related device, or imitation tobacco product. This includes products or paraphernalia displaying tobacco industry brand; or
- 5. ~~using~~ or consuming a tobacco product on District premises, ~~except:~~
- 6.5. ~~or at outdoor areas including, but not limited to, an open-air stadium, on Saturdays, Sundays, and other days on which there are no regularly scheduled school hours, or a District function.~~

- ~~a. after 6 p.m. on days during which there are regularly scheduled school hours;~~

Violating these standards will subject an employee to discipline, including discharge.

It shall be a violation of this Policy for an employee to solicit or accept any contributions, gifts, money, curricula, or materials from the tobacco industry or from any tobacco products shop for use at a District premises or District function. This includes, but is not limited to, donations, money for sponsorship, advertising material, alleged educational materials, promotions, loans, scholarships, or support for equipment, uniforms, sports, or training facilities. It shall also be a violation of this Policy to participate in any type of service funded by the tobacco industry on District premises or at a District function.

If a reasonable suspicion exists that an employee is under the influence, the Superintendent or designee may direct the employee to submit to a drug test or breathalyzer. If the employee refuses, the employee may be subject to discipline, including discharge, based on the District's observations.

D. It shall not be a violation of this policy:

1. for commercial tobacco products, tobacco-related devices, imitation tobacco products, or lighters to be included in an instructional or work-related activity in the District school buildings if the activity is conducted by a staff member or an approved visitor and the activity does not include smoking, chewing, or otherwise ingesting the product;
2. for a person to possess or provide tobacco, tobacco-related devices, imitation tobacco products, or lighters to any other person as part of an indigenous practice used by Native communities for spiritual and medicinal purposes. It shall not be a violation of this policy to use tobacco, tobacco-related devices, imitation tobacco products, or lighters as part of an educational experience related to traditional or sacred tobacco practices that has been approved by administrators;
3. to use or possess a product that has been approved by the U.S. Food and Drug Administration for sale as a tobacco cessation product, as a nicotine dependence product, or for other medical purposes, and is being marketed and sold solely for such an approved purpose. [National, or]
4. to use or possess a tobacco product on District premises at outdoor areas including, but not limited to, an open-air stadium during either the following time periods:
 - a. on Saturdays, Sundays, and other days on which there are no regularly scheduled school hours, or

b. after 6 p.m. on days during which there are regularly scheduled school hours.]

Formatted: Highlight

E. Support

Administrators shall consult with the local public health department or other appropriate health and allied community-based organizations to provide students, staff, and administrators with information and access to support systems, programs, and services to encourage them to abstain from the use of commercial tobacco products. Administrators shall identify and offer evidence-based programs and services for individuals that use commercial tobacco products to support them in complying with this policy.

F. Notice

The District shall provide notice of this policy in staff handbooks, through orientations and employee or staff training, and when offering employment.

D-G. [Optional: Reporting Requirements for Transportation Employees Subject to Omnibus Transportation Employee Testing Act]

An employee subject to the Omnibus Transportation Employee Testing Act must notify the Superintendent or designee of any criminal drug conviction for a violation occurring in the workplace no later than 5 calendar days after that conviction. Upon receiving notice of an employee's conviction of a criminal drug violation occurring in the workplace, the Board or designee must take appropriate action within 30 calendar days.]

Legal authority: 20 USC 7101 et seq.; 41 USC 8101 et seq.; 42 USC 12101 et seq.; Schedules I-V of Chapter 13 of the Controlled Substances Act, 21 USC 812; 29 USC 701 et seq.; MCL 37.1211; Schedules 1-5 of the Michigan Uniform Controlled Substances Act, MCL 333.7201 et seq.; MCL 380.11a, 380.601a; MCL 436.1101 et seq.; MCL 750.473.

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4216 *Personal Communications Devices*

"Personal communications device" includes employee-owned cell phones, computers, tablets, or any other device that is capable of, but not limited to, text messaging, voice communication, downloading applications, entertainment, navigation, accessing the internet, sending and receiving photos and videos, or producing email. Employee use of personal communications devices during the work day, including school-sponsored activities, and to conduct school-related business, is limited as follows:

- A. except in emergencies, an employee's use of a personal communications device shall not interfere with instructional activities or work-related duties. Employees taking an authorized break may use a personal communications device in a manner that does not disrupt the District's operations or violate the confidentiality of students or others;
- B. employees shall not use a personal communications device to access inappropriate content or engage in unlawful activities while on duty, on District property, or attending a District-related event;
- C. employees must not use a personal communications device to inappropriately communicate with other employees, students, or Parents;
- D. employees must ensure that the District's records and files, including confidential student information, are only maintained on District-provided technology and that confidentiality is maintained. District records and files must not be stored on a personal communications device;
- E. employees recognize that when a personal communications device accesses the District's network, the employee's use may become subject to the District's Acceptable Use Policy;
- F. employees may not use a personal communications device to record communications or images during the work or school day or at a school-sponsored event other than a public performance or sporting event, unless the employee has received permission from the Superintendent or designee. Dissemination of any recording is prohibited unless the Superintendent or designee approves that action in writing; or
- G. unauthorized recording of communications or images of students, Parents, co-workers, or non-public meetings is prohibited unless there is an educational purpose to do so, and may result in discipline, including discharge.

Legal authority: MCL 380.11a(3), 380.601a

Date adopted: August 15, 2022

Date revised: August 19, 2024

Date revised: July 20, 2026

Series 4000: District Employment

4200 Employee Conduct and Ethics

4216 Personal Communication~~s~~ Devices

"Personal communication~~s~~ devices" includes~~s~~ employee-owned cell phones, computers, tablets, or any other device that is capable of, but not limited to, text messaging, voice communication, downloading applications, entertainment, navigation, accessing the internet, sending and receiving photos and videos, or producing email.~~enables an employee to access the internet or engage in communications through an application, social media, or any other communication method.~~ Employee use of personal communication~~s~~ devices during the work day, including school-sponsored activities, and to conduct school-related business, is limited as follows:

- A. except in emergencies, an employee's use of a personal communication~~s~~ devices shall not interfere with instructional activities or work-related duties. Employees taking an authorized break may use a personal communication~~s~~ devices in a manner that does not disrupt the District's operations or violate the confidentiality of students or others;
- B. employees shall not use a personal communication~~s~~ devices to access inappropriate content or engage in unlawful activities while on duty, on District property, or attending a District-related event;
- C. employees must not use a personal communication~~s~~ devices to inappropriately communicate with other employees, students, ~~and/or~~ Parents;
- D. employees must ensure that the District's records and files, including confidential student information, are only maintained on District-provided technology and that confidentiality is maintained. District records and files must not be stored on a personal communication~~s~~ device;
- E. employees recognize that when a personal communication~~s~~ device accesses the District's network, the employee's use may become subject to the District's Acceptable Use Policy;
- F. employees may not use ~~their~~ a personal communication~~s~~ devices to record communications or images during the work or school day or at a school-sponsored event other than a public performance or sporting event, unless the employee has received permission from the Superintendent or designee. Dissemination of any recording is prohibited unless the Superintendent or designee approves that action in writing; or
- G. unauthorized recording of communications or images of students, Parents, co-workers, or non-public meetings is prohibited [Optional: unless there is an educational purpose to do so.] and may result in discipline, including discharge.

Legal authority: MCL 380.11a(3), 380.601a

Date adopted:

Date revised:

Series 4000: District Employment

4500 Administrators/Supervisors

4508 Administrator Non-Renewal

A. Administrators Subject to Revised School Code Section 1229(2)

Administrator contract non-renewal may be subject to Revised School Code Section 1229(2) depending on the person's responsibilities, duties, and certification. If the non-renewal of an Administrator is subject to Revised School Code Section 1229(2), this Policy shall be implemented consistent with that statute.

"Non-renewal" is an action to discontinue an employment contract at contract expiration. Termination during the term of an existing employment contract is addressed in Policy 4507.

If Revised School Code Section 1229(2) applies, the non-renewal of an Administrator's individual employment contract must be preceded by a notice to the employee that the Board is considering non-renewal. Written notice of consideration of non-renewal must be given to the Administrator at least 90 calendar days before the expiration date of the Administrator's contract. The Administrator will be provided notice of the Board meeting at which the consideration of non-renewal will be reviewed and may request an open or closed session, where appropriate. The Board must act in open session on the recommendation to consider non-renewal.

The Superintendent or designee will notify the Administrator of the Board's decision to consider non-renewal, including a written statement of the reason(s). The employee may request to meet with a majority of the Board to discuss the reason(s) in open or closed session, where appropriate. The meeting with the majority of the Board to discuss the reason(s) it is considering non-renewal must take place following notice to the administrator of the consideration of non-renewal and before any action of non-renewal.

There must be a minimum of 30 calendar days between the time that the administrator is provided written notice that the Board is considering non-renewal, including a statement of the reason(s) for consideration of non-renewal, and the Board's action to renew or non-renew the administrator's individual employment contract. The resolution and notice of non-renewal must be provided to the administrator not less than 60 calendar days before the expiration date of the administrator's individual employment contract.

If the non-renewal is based on a reduction in personnel and not for a performance reason, the Board's review and action must take place in open session.

If the employee holds tenure rights as a classroom teacher and the District seeks to terminate those tenure rights, the District will comply with the Teachers' Tenure Act.

B. Non-Renewal of a Supervisor or Director

A Supervisor's or Director's contract may be non-renewed in accordance with the applicable individual employment contract or collective bargaining agreement. If the Supervisor or Director is not subject to an individual employment contract or collective bargaining agreement, the Superintendent or designee will present a recommendation of non-renewal to the Board at least 60 calendar days before June 30, stating the reason(s) for the recommendation. Advance written notice of the recommendation, the time, date, and location of the Board meeting, and the option for closed session deliberation will be provided to the Supervisor or Director.

Legal authority: MCL 380.1229

Date adopted: August 15, 2022

Date revised: July 20, 2026

Series 4000: District Employment

4500 Administrators/Supervisors

4508 Administrator Non-Renewal

A. Administrators Subject to Revised School Code Section 1229(2)

Administrator contract non-renewal may be subject to Revised School Code Section 1229(2) depending on the person's responsibilities, duties, and certification. If the non-renewal of an Administrator is subject to Revised School Code Section 1229(2), this Policy shall be implemented consistent with that statute.

"Non-renewal" is an action to discontinue an employment contract at contract expiration. Termination during the term of an existing employment contract is addressed in Policy 4507.

If Revised School Code Section 1229(2) applies, the non-renewal of an Administrator's individual employment contract must be preceded by a notice to the employee that the Board is considering non-renewal. Written notice of consideration of non-renewal must be given to the Administrator at least 90 calendar days before the expiration date of the Administrator's contract. The Administrator will be provided notice of the Board meeting at which the consideration of non-renewal will be reviewed and may request an open or closed session, where appropriate. The Board must act in open session on the recommendation to consider non-renewal.

The Superintendent or designee will notify the Administrator of the Board's decision to consider non-renewal, including a written statement of the reason(s). The employee may request to meet with a majority of the Board to discuss the reason(s) in open or closed session, where appropriate. The meeting with the majority of the Board to discuss the reason(s) it is considering non-renewal must take place following notice to the administrator of the consideration of non-renewal and before any action of non-renewal.

There must be a minimum of 30 calendar days between the time that the administrator is provided written notice that the Board is considering non-renewal, including a statement of the reason(s) for consideration of non-renewal, and the Board's action to renew or non-renew the administrator's individual employment contract. The resolution and notice of non-renewal must be provided to the administrator not less than 60 calendar days before the expiration date of the administrator's individual employment contract.

If the non-renewal is based on a reduction in personnel and not for a performance reason, the Board's review and action must take place in open session.



If the employee holds tenure rights as a classroom teacher and the District seeks to terminate those tenure rights, the District will comply with the Teachers' Tenure Act.

B. Non-Renewal of a Supervisor or Director

A Supervisor's or Director's contract may be non-renewed in accordance with the applicable individual employment contract or collective bargaining agreement. ~~Absent any contractual guidance~~ Self the Supervisor or Director is not subject to an applicable individual employment contract or collective bargaining agreement, the Superintendent or designee will present a recommendation of non-renewal ~~will be presented~~ to the Board at least [] calendar days before ~~the contract expiration~~ June 30, stating the reason(s) for the recommendation. Advance written notice of the recommendation, the time, date, and location of the Board meeting, and the option for closed session deliberation will be provided to the Supervisor or Director.

Legal authority: MCL 380.1229

Date adopted:

Date revised:

Series 4000: District Employment

4600 The Superintendent

4602 Hiring

The Board will determine and select the best candidate to serve as the Superintendent, based on qualifications, experience, demonstrated capabilities, and other relevant factors as determined by the Board. The Board may enlist professional consultants, employees, community members, or others to assist with the recruitment and selection process.

Qualified candidates will possess and maintain certifications, permits, and approvals required by federal and state law for the office of Superintendent. The hiring process will comply with the Michigan Open Meetings Act.

Before hiring the selected candidate, an offer of employment will be conditioned on successful completion of a background check as described in Policy 4205.

The Board should consult with legal counsel when drafting the Superintendent's employment contract.

The Superintendent's employment contract shall not exceed five years in duration. If a Superintendent vacates the position before a new Superintendent is selected, the Board shall appoint an interim Superintendent to oversee operations until a new Superintendent is selected. Hiring decisions shall be based on qualifications, skills, knowledge, abilities, education, certifications/licenses, experience, demeanor, and other criteria the Board may deem relevant.

Legal authority: MCL 15.261 et seq.; MCL 380.1229(1), 380.1536

Date adopted: August 15, 2022

Date revised: July 20, 2026

Series 4000: District Employment

4600 The Superintendent

4602 Hiring

The Board will determine and select the best candidate to serve as the Superintendent, based on qualifications, experience, ~~and demonstrated capabilities.~~ and other relevant factors as determined by the Board. The Board may enlist professional consultants, employees, community members, or others to assist with the recruitment and selection process.

Qualified candidates will possess and maintain certifications, permits, and approvals required by federal and state law for the office of Superintendent. The hiring process will comply with the Michigan Open Meetings Act.

Before hiring the selected candidate, an offer of employment will be conditioned on successful completion of a background check as described in Policy 4205.

The Board should consult with legal counsel when drafting the Superintendent's employment contract.

The Superintendent's employment contract shall not exceed five years in duration. If a Superintendent vacates the position before a new Superintendent is selected, the Board shall appoint an interim Superintendent to oversee operations until a new Superintendent is selected. Hiring decisions shall be based on qualifications, skills, knowledge, abilities, education, certifications/licenses, experience, demeanor, and other criteria the Board may deem relevant.

Legal authority: MCL 15.261 et seq.; MCL 380.1229(1), 380.1536

Date adopted:

Date revised: