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/guardians~~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/guardians~~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;

~~7.~~8. maintaining confidential information, including student, medical, personnel, financial, and security information, as protected by statute;

~~8.~~9. appropriately using District funds, resources, and technology;

~~9.~~10. maintaining consistent and reliable work attendance, unless excused by the employee's supervisor or the Superintendent or designee, as applicable;

~~10.~~11. engaging in activities or behaviors that enhance the operational and instructional environment;

~~11.~~12. professionally communicating with students, ~~parents/guardians~~Parents, colleagues, Board members, and community members, including through electronic means;

~~12.~~13. Completing time and effort reporting under 4201-AG.

~~13.~~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

~~14.~~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 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. 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/guardian~~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 prior ~~parent/guardian~~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/guardian~~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/guardian~~Parent;

17. going to a student's home when the student's ~~parent/guardian~~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. ~~Employees suspecting~~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

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 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. 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 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.

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: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4202 Children's Protective Services (CPS) and Adult Protective Services (APS) Reporting and Student Safety and Welfare

During the performance of their duties, employees must exercise due care for the safety and welfare of the District's students.

A. Required Reports to CPS, APS, District administration, and Michigan State Police

1. A reporter must: (a) promptly notify the Superintendent or designee and the building principal of the report; and (b) submit an electronic or written report to CPS or APS within the statutory timeframe. Failure to make an immediate report or follow-up with an electronic or written report may result in discipline, including discharge, as well as criminal or civil penalties. CPS and APS may be contacted at 855-444-3911 or www.michigan/gov/mdhhs.

   Administrators, teachers, counselors, social workers, psychologists, nurses, physical therapists, physical therapist assistants, occupational therapists, athletic trainers, and others identified as mandatory reporters pursuant to Michigan's Child Protection Law must *immediately* report all instances of suspected child abuse or neglect to CPS. Other employees are also expected to make reports to CPS of suspected child abuse or neglect.

   School employees who suspect or have reasonable cause to believe that a vulnerable adult was or is being subjected to abuse, neglect, or exploitation must *immediately* report the matter to APS. A vulnerable adult means a person 18 years of age or older who is unable to protect themselves from abuse, neglect, or exploitation because of a mental or physical impairment or because of advanced age.

2. Employees must promptly report to the building principal or the Superintendent or designee any instances of injury (accidental or intentional), violence, threats of violence, self-harm, hazards, or any other situation that endangers student safety and welfare or raises reasonable concerns as to the safety of students.

3. Employees must promptly report to the building principal or the Superintendent or designee incidents of student bullying and crimes or attempted crimes involving physical violence, gang-related activity, illegal possession of a controlled substance or controlled substance analogue, or other intoxicant, trespassing, and property crimes, including theft and vandalism.

   Within 24 hours of an alleged incident, an administrator must make an appropriate report to the Michigan State Police as required by law.

B. Student Safety and Welfare

1. Employees will maintain control and supervision of students to ensure student safety and will take appropriate action if the employee observes an unsafe or dangerous situation.

2. Employees will treat students with respect and maintain appropriate professional boundaries with students both in and out of school. Employees must avoid conduct with students that potentially creates the appearance of an unprofessional, unethical, or inappropriate relationship. Romantic relationships between employees and students are prohibited regardless of the student's age, including following graduation where the relationship arises out of an employee-student relationship.

3. An employee will not assess, diagnose, prescribe, or provide therapy or counseling services to a student unless: (a) the employee is appropriately certified or licensed under Michigan law; and (b) the services are within the employee's job duties. An employee will direct students in need of these services to the appropriate District employee or community resource.

4. Employees will comply with and respect confidentiality of student records and privacy rights, including not posting student information or images online without prior authorization from the employee's supervisor.

5. Employees will not interfere with or adversely impact a ~~parent's/guardian's~~Parent's right to determine and direct their student's care, wellbeing, teaching, and education.

6. [Optional: Pursuant to the state's 2013 Task Force on the Prevention of Sexual Abuse of Children, the Board authorizes the Superintendent or designee to consider and implement all of the following:

   - age-appropriate, evidence-based curriculum and instruction for students in grades pre-K to 5 concerning child sexual abuse awareness and prevention;
   - training for District personnel on child sexual abuse, including but not limited to, training on supportive, appropriate response to disclosure of abuse;
   - providing educational information to ~~parents/guardians~~Parents on the warning signs of a child being sexually abused and information on needed assistance, referral, or resources;
   - available counseling and resources for students affected by sexual abuse;
   - emotional and educational support for a students affected by sexual abuse; and
   - a review of the system to educate and support personnel who are legally required to report child abuse or neglect.]

Legal authority: MCL 380.10, 380.1308, 380.1308a, 380.1310a, 380.1505; MCL ~~388.1766;~~400.11 et seq.; MCL 722.621 et seq.

Dated adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4202 Children's Protective Services (CPS) and Adult Protective Services (APS) Reporting and Student Safety and Welfare

During the performance of their duties, employees must exercise due care for the safety and welfare of the District's students.

A. Required Reports to CPS, APS, District administration, and Michigan State Police

1. A reporter must: (a) promptly notify the Superintendent or designee and the building principal of the report; and (b) submit an electronic or written report to CPS or APS within the statutory timeframe. Failure to make an immediate report or follow-up with an electronic or written report may result in discipline, including discharge, as well as criminal or civil penalties. CPS and APS may be contacted at 855-444-3911 or www.michigan.gov/mdhhs.

   Administrators, teachers, counselors, social workers, psychologists, nurses, physical therapists, physical therapist assistants, occupational therapists, athletic trainers, and others identified as mandatory reporters pursuant to Michigan's Child Protection Law must *immediately* report all instances of suspected child abuse or neglect to CPS. Other employees are also expected to make reports to CPS of suspected child abuse or neglect.

   School employees who suspect or have reasonable cause to believe that a vulnerable adult was or is being subjected to abuse, neglect, or exploitation must *immediately* report the matter to APS. A vulnerable adult means a person 18 years of age or older who is unable to protect themselves from abuse, neglect, or exploitation because of a mental or physical impairment or because of advanced age.

2. Employees must promptly report to the building principal or the Superintendent or designee any instances of injury (accidental or intentional), violence, threats of violence, self-harm, hazards, or any other situation that endangers student safety and welfare or raises reasonable concerns as to the safety of students.

3. Employees must promptly report to the building principal or the Superintendent or designee incidents of student bullying and crimes or attempted crimes involving physical violence, gang-related activity, illegal possession of a controlled substance or controlled substance analogue, or other intoxicant, trespassing, and property crimes, including theft and vandalism.

   Within 24 hours of an alleged incident, an administrator must make an appropriate report to the Michigan State Police as required by law.

B. Student Safety and Welfare

1. Employees will maintain control and supervision of students to ensure student safety and will take appropriate action if the employee observes an unsafe or dangerous situation.

2. Employees will treat students with respect and maintain appropriate professional boundaries with students both in and out of school. Employees must avoid conduct with students that potentially creates the appearance of an unprofessional, unethical, or inappropriate relationship. Romantic relationships between employees and students are prohibited regardless of the student's age, including following graduation where the relationship arises out of an employee-student relationship.

3. An employee will not assess, diagnose, prescribe, or provide therapy or counseling services to a student unless: (a) the employee is appropriately certified or licensed under Michigan law; and (b) the services are within the employee's job duties. An employee will direct students in need of these services to the appropriate District employee or community resource.

4. Employees will comply with and respect confidentiality of student records and privacy rights, including not posting student information or images online without prior authorization from the employee's supervisor.

5. Employees will not interfere with or adversely impact a Parent's right to determine and direct their student's care, wellbeing, teaching, and education.

6. Reserved Legal authority: MCL 380.10, 380.1308, 380.1308a, 380.1310a, 380.1505; MCL 400.11 et seq.; MCL 722.621 et seq.

Dated adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4203-AG Corporal Punishment and Limited Use of Reasonable Force

A list of alternatives to corporal punishment includes the following:

- provide direct instruction to students in social skills and problem-solving strategies;
- use positive reinforcement to teach and maintain the use of appropriate problem-solving and social skills;
- use social reinforcers, such as teacher feedback and other self-esteem enhancing activities, to support and maintain the use of problem-solving and social skills;
- apply logical consequences that will teach students personal responsibility for their actions (e.g., losing the privilege of participating in special school activities);
- consider the use of time out, which may allow students to learn to take control of their actions and, ultimately, in conjunction with instruction in social skills, to cease their undesirable behavior;
- employ problem-solving classroom meetings and/or school assemblies with honest discussion of problems to encourage student ownership of and responsibility for solutions;
- establish a variety of strategies for communicating with Parents;
- establish contractual agreements that clearly outline consequences with students and their Parents to enhance the development of self-control behavior;
- establish an in-school suspension program, supervised by a responsible adult, in which the student performs curricula-related activities;
- when necessary, refer students to a counselor, social worker, or psychologist at the local or intermediate level and coordinate services with other units of state government (e.g., public health, social services, mental health). Also, seek assistance from private institutions or agencies with appropriate services;
- evaluate and arrange appropriate curriculum and adequate support for students who need academic acceleration, special education, alternative education, or services for achieving English proficiency;
- consider and take action, in accordance with the applicable student code of conduct and due process of law, when disruptive behavior occurs; or
- consider the use of suspensions or expulsions only after other alternatives have been considered.

The Board adopts the above list. District administration will distribute this list to each employee, volunteer, and contractor.

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4203-AG Corporal Punishment and Limited Use of Reasonable Force

A list of alternatives to corporal punishment includes the following:

- provide direct instruction to students in social skills and problem-solving strategies;
- use positive reinforcement to teach and maintain the use of appropriate problem-solving and social skills;
- use social reinforcers, such as teacher feedback and other self-esteem enhancing activities, to support and maintain the use of problem-solving and social skills;
- apply logical consequences that will teach students personal responsibility for their actions (e.g., losing the privilege of participating in special school activities);
- consider the use of time out, which may allow students to learn to take control of their actions and, ultimately, in conjunction with instruction in social skills, to cease their undesirable behavior;
- employ problem-solving classroom meetings and/or school assemblies with honest discussion of problems to encourage student ownership of and responsibility for solutions;
- establish a variety of strategies for communicating with Parents;
- establish contractual agreements that clearly outline consequences with students and their Parents to enhance the development of self-control behavior;
- establish an in-school suspension program, supervised by a responsible adult, in which the student performs curricula-related activities;
- when necessary, refer students to a counselor, social worker, or psychologist at the local or intermediate level and coordinate services with other units of state government (e.g., public health, social services, mental health). Also, seek assistance from private institutions or agencies with appropriate services;
- evaluate and arrange appropriate curriculum and adequate support for students who need academic acceleration, special education, alternative education, or services for achieving English proficiency;
- consider and take action, in accordance with the applicable student code of conduct and due process of law, when disruptive behavior occurs; or
- consider the use of suspensions or expulsions only after other alternatives have been considered.

The Board adopts the above list. District administration will distribute this list to each employee, volunteer, and contractor.

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4204 Confidentiality of Student Information

Employees must maintain and protect the confidentiality of student information and student education records (as defined in Policy 5309) and recognize ~~parent/guardian~~Parent rights to student information about their minor child(ren).

Employees must not disclose to third parties confidential student information or records, medical information, performance records, or behavior records unless appropriately authorized. This Policy prohibits disclosure to employees who do not have a legitimate educational interest in the student record.

Disclosure is appropriately authorized with a written release from the ~~parent/guardian~~Parent or student 18 years or older in accordance with the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), implementing regulations, and state law.

Employees who receive a subpoena seeking disclosure of student records or other confidential information must immediately notify the Superintendent or designee. Employees must not speak with an attorney who does not represent the District about a student without approval from the Superintendent or designee.

Legal authority: 20 USC 1232g, 1415(b); 34 CFR 99; MCL 380.1136; MCL 600.2165

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4204 Confidentiality of Student Information

Employees must maintain and protect the confidentiality of student information and student education records (as defined in Policy 5309) and recognize Parent rights to student information about their minor child(ren).

Employees must not disclose to third parties confidential student information or records, medical information, performance records, or behavior records unless appropriately authorized. This Policy prohibits disclosure to employees who do not have a legitimate educational interest in the student record.

Disclosure is appropriately authorized with a written release from the Parent or student 18 years or older in accordance with the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), implementing regulations, and state law.

Employees who receive a subpoena seeking disclosure of student records or other confidential information must immediately notify the Superintendent or designee. Employees must not speak with an attorney who does not represent the District about a student without approval from the Superintendent or designee.

Legal authority: 20 USC 1232g, 1415(b); 34 CFR 99; MCL 380.1136; MCL 600.2165

Date adopted: August 15, 2022

Date revised: August 19, 2024

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 ~~Guidance~~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, ~~volunteers,~~ 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 [ ] [Note: add the position of individual. Delete this note upon designation.], a District employee, who: (1) is an authorized user, (2) has completed ~~fingerprinting and~~ a fingerprint-based background check ~~have~~ as required, (3) has been found appropriate to have access to ~~background checks~~CHRI, and (4) is directly involved in evaluating ~~person's~~an individual's qualifications for employment. ~~Delete this note upon designation.]~~ 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:

~~b.~~a. compliance with these regulations and laws;

~~c.~~b. personnel security screening procedures are followed under this administrative guideline;

~~d.~~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;

~~d.~~e. only approved District employees have access to and are using the information in compliance with the law;

~~e.~~f. compliance with this administrative guideline; ~~and~~

g. that the MSP Information Security Officer (ISO) is promptly informed of any security ~~breach(es).~~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

~~f.~~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:

~~b.~~a. ~~how~~ District equipment ~~is~~ connected to the MSP system; and

~~c.~~b. who is using ~~the MSP-approved equipment~~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 ~~twenty-four (~~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 ~~twenty-four (~~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, ~~unless the personally owned devices are approved,~~ 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 ~~be~~ (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:

~~b.~~a. at least eight (8) characters;

~~c.~~b. not consisting of only a proper noun or word found in a dictionary;

~~d.~~c. not similar or identical to the username;

~~e.~~d. not be displayed while entered or transmitted outside of the physically secure location or controlled area;

~~f.~~e. expires every ninety (90) days; and

~~g.~~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~~, following the template provided~~ about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on ~~the MSP website,~~ 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 ~~six (6) months of authorization and every two (2) years thereafter.~~ 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 ~~the~~ training.

5. CHRI Dissemination

The District must maintain a record of any CHRI dissemination to another authorized agency for all dissemination outside the CHRISS 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 ~~be tracked using the~~ report ~~the~~such incidents to the superintendent and MSP ~~provides on its website https://www.michigan.gov/msp/0,4643,7-123-72297_24055-332662--,00.html~~ISO using the MSP CJIS-016 reporting from. 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. ~~AA~~ [add company name of building a a m] building alarm or video surveillance will monitor for physical or	Electronic intrusions will be monitored by the virus and malware/spyware detection.

	unauthorized intrusions. The building must be locked at night.	
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 ~~apply~~take place:

~~b.~~ Notice: Personnel will notify the LASO ~~will be notified~~ immediately~~;~~

a. or no later than one hour after the incident was discovered.

~~c.~~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.

~~c.~~f. Records: The LASO or appointed authorized ~~used~~user will record all necessary information regarding the breach, the District's response to the breach, and who was involved in taking response measures~~;~~.

~~e. the LASO will file the incident report with the MSP; and~~

g. ~~when~~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 handing 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.

~~e.~~j. Legal Action: When such incident results in legal action (either civil or criminal) against a person or the District, ~~evidence~~the local law enforcement agency shall be ~~collected, retained~~contacted to collect, retain, and ~~presented~~present evidence, according to the evidentiary rules of the appropriate jurisdiction(s).

~~2.~~E. ~~Mobile Device~~ Incident ~~Handling~~Response Support and Plan

1. Response Support Resource: The District will~~, in addition~~ provide a response support resource that offers advice and assistance to ~~the~~ system users for handling ~~procedure~~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 handing 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:

b. agency and system-level audit and accountability policy

1. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and

2. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

c. 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 logging in ~~the table above,~~ 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:

      1. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

      2. 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 ~~additional procedures for mobile devices to reduce the risk of unauthorized access to CHRI.~~ process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

~~When a device is lost, the District will document and indicate how long the device has been lost. For a lost device, the District will report if the owner believed the device was locked, unlocked, or could not verify the device's locked state. For a total loss of a device (unrecoverable), the District will report if CHRI was stored on the device, whether it was locked or unlocked, and whether the District can track or wipe the device remotely. The District will report any compromise of a device while still in the owner's possession and any compromise outside of the United States.~~

~~Adoption date:~~

h. ~~Revised date:~~ align account management processes with personnel termination and transfer processes.

I. Access Enforcement

1. The District will:

a. enforce approved authorization for logical access to information and system resources will be enforced in accordance with applicable access control policies; and

b. provide automated or manual processes to enable individuals to access elements of their personally identifiable information.

J. Information Flow Enforcement

1. 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

1. The District will:

a. identify and document separation of duties based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI; and

b. 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:

1. established system accounts, configured access authorizations, set events to be audited, set intrusion detection parameters, and other security functions; and

2. 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

1. 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; and

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.

1. The District establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

2. The District authorizes each type of remote access to the system prior to allowing such connections.

3. The District employs automated mechanisms to monitor and control remote access methods.

4. The District implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

5. The District routes remote access through authorized and managed network access control points.

6. The District 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.

7. The District documents the rational 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)

Date adopted:

Date revised:

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 Administrative Assistant, 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 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 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 CHRISS 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 from. 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 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 Sherriff / Grand Rapids Township Police] 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 [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 handing

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 handing 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:

   b. agency and system-level audit and accountability policy

      1. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and

      2. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

   c. 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 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:

      1. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

      2. 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

1. The District will:

a. enforce approved authorization for logical access to information and system resources will be enforced in accordance with applicable access control policies; and

b. provide automated or manual processes to enable individuals to access elements of their personally identifiable information.

J. Information Flow Enforcement

1. 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

1. The District will:

a. identify and document separation of duties based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI; and

b. 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:

        1. established system accounts, configured access authorizations, set events to be audited, set intrusion detection parameters, and other security functions; and

        2. 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

1. 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; and

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.

1. The District establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

2. The District authorizes each type of remote access to the system prior to allowing such connections.

3. The District employs automated mechanisms to monitor and control remote access methods.

4. The District implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

5. The District routes remote access through authorized and managed network access control points.

6. The District 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.

7. The District documents the rational 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)

Date adopted: August 19, 2024

Date revised:

4200 Employee Conduct and Ethics

4206 Employment Contracts

Professional Staff, Administrators/Supervisors, and the Superintendent, as defined in Policies 4401, 4501, and 4601, will be employed by an individual employment contract and any applicable collective bargaining agreement. Non-Exempt Staff, as defined in Policy 4301, will be employed at-will unless governed by a collective bargaining agreement or individual employment contract specifying another standard of employment security.

Employment contracts will comply with applicable laws, and regulations. The President or Superintendent, as applicable, should consult with Board legal counsel about contract terms and requirements to ensure compliance with state and federal law.

A. Authority

The President is authorized to execute the Superintendent's contract on behalf of the Board upon Board approval of the contract. Teacher contracts must be approved by the Board and signed on behalf of the District by a majority of the Board, the President and Secretary, or the Superintendent or designee. The Superintendent is authorized to execute employment contracts for non-exempt staff and temporary and substitute employees on the Board's behalf or upon Board approval, where necessary.

B. General Requirements

Individual employment contracts required or permitted under this Policy may contain at least the following, as applicable to the category of employment:

1. employee name;
2. term of employment;
3. annual salary or hourly rate;
4. merit pay and annual evaluation for teachers and required administrators;
5. job title;
6. number of work days and general hours of work;
7. certification and licensing requirements;
8. benefits (health insurance, leave time, etc.);
9. reduction in force and recall;
10. discipline, discharge, and transfer during the contract term;

11. date and employee signature;

12. date and signature of authorized District representative; ~~and~~

13. an appeal process concerning the evaluation process and rating received as required by Revised School Code Sections 1249 (K-12 certified teachers of record) and 1249b (instructional administrators and the Superintendent); and

~~13.~~14. other terms as necessary to serve the District's interests or that are legally required.

Administrative contracts must contain a provision prohibiting an Administrator from engaging in conduct involving moral turpitude and a provision allowing the Board to void the contract if the Administrator violates the moral turpitude provision.

C. Specific Requirements

Professional Staff, Administrator, and Superintendent contracts must comply with the following, as applicable:

1. Superintendent

   The contract term will not exceed 5 years, as required by Revised School Code Section 1229.

2. Administrators

   For Administrators subject to Revised School Code Section 1229, the contract term will not exceed 3 years and the contract will automatically terminate if the Administrator does not hold the required certification. The Administrator will not have tenure in the administrative position.

   The Superintendent or designee will ensure that Administrator contracts are consistent with any applicable collective bargaining agreement. The term Administrator includes instructional Supervisors or Directors.

3. Non-Instructional Supervisors or Directors

   Unless otherwise required by law, Non-Instructional Supervisors or Directors are not required to hold an Administrator certificate and may be subject to an individual employment contract for up to 3 years.

4. Professional Staff

   The Superintendent or designee will ensure that all Professional Staff contracts are consistent with any applicable collective bargaining agreement. Individual teacher contracts will comply with Revised School Code Section 1231. If a teacher seeks appointment to an extracurricular position, the District may enter into a separate written contract for the extracurricular position.

D. Collective Bargaining Agreements

The Board, with the Superintendent or designee, will determine who will represent the Board in labor negotiations. The designated negotiator(s) may sign tentative agreements during bargaining; however, the final agreement is subject to ratification by the Board. Collective bargaining agreements may be reviewed by legal counsel before bargaining begins.

Legal authority: MCL 380.11a(3), 380.601(d), 380.623(1)(b), 380.634, 380.1229, 380.1231, 380.1246, 380.1249, 380.1249b

Date adopted:

Date revised:

4200 Employee Conduct and Ethics

4206 Employment Contracts

Professional Staff, Administrators/Supervisors, and the Superintendent, as defined in Policies 4401, 4501, and 4601, will be employed by an individual employment contract and any applicable collective bargaining agreement. Non-Exempt Staff, as defined in Policy 4301, will be employed at-will unless governed by a collective bargaining agreement or individual employment contract specifying another standard of employment security.

Employment contracts will comply with applicable laws, and regulations. The President or Superintendent, as applicable, should consult with Board legal counsel about contract terms and requirements to ensure compliance with state and federal law.

A. Authority

The President is authorized to execute the Superintendent's contract on behalf of the Board upon Board approval of the contract. Teacher contracts must be approved by the Board and signed on behalf of the District by a majority of the Board, the President and Secretary, or the Superintendent or designee. The Superintendent is authorized to execute employment contracts for non-exempt staff and temporary and substitute employees on the Board's behalf or upon Board approval, where necessary.

B. General Requirements

Individual employment contracts required or permitted under this Policy may contain at least the following, as applicable to the category of employment:

1. employee name;
2. term of employment;
3. annual salary or hourly rate;
4. merit pay and annual evaluation for teachers and required administrators;
5. job title;
6. number of work days and general hours of work;
7. certification and licensing requirements;
8. benefits (health insurance, leave time, etc.);
9. reduction in force and recall;
10. discipline, discharge, and transfer during the contract term;

11. date and employee signature;

12. date and signature of authorized District representative;

13. an appeal process concerning the evaluation process and rating received as required by Revised School Code Sections 1249 (K-12 certified teachers of record) and 1249b (instructional administrators and the Superintendent); and

14. other terms as necessary to serve the District's interests or that are legally required.

Administrative contracts must contain a provision prohibiting an Administrator from engaging in conduct involving moral turpitude and a provision allowing the Board to void the contract if the Administrator violates the moral turpitude provision.

C. Specific Requirements

Professional Staff, Administrator, and Superintendent contracts must comply with the following, as applicable:

1. Superintendent

   The contract term will not exceed 5 years, as required by Revised School Code Section 1229.

2. Administrators

   For Administrators subject to Revised School Code Section 1229, the contract term will not exceed 3 years and the contract will automatically terminate if the Administrator does not hold the required certification. The Administrator will not have tenure in the administrative position.

   The Superintendent or designee will ensure that Administrator contracts are consistent with any applicable collective bargaining agreement. The term Administrator includes instructional Supervisors or Directors.

3. Non-Instructional Supervisors or Directors

   Unless otherwise required by law, Non-Instructional Supervisors or Directors are not required to hold an Administrator certificate and may be subject to an individual employment contract for up to 3 years.

4. Professional Staff

   The Superintendent or designee will ensure that all Professional Staff contracts are consistent with any applicable collective bargaining agreement. Individual teacher contracts will comply with Revised School Code Section 1231. If a teacher seeks appointment to an extracurricular position, the District may enter into a separate written contract for the extracurricular position.

D. Collective Bargaining Agreements

The Board, with the Superintendent or designee, will determine who will represent the Board in labor negotiations. The designated negotiator(s) may sign tentative agreements during bargaining; however, the final agreement is subject to ratification by the Board. Collective bargaining agreements may be reviewed by legal counsel before bargaining begins.

Legal authority: MCL 380.11a(3), 380.601(d), 380.623(1)(b), 380.634, 380.1229, 380.1231, 380.1246, 380.1249, 380.1249b

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4207 Third-Party Contracting

This Policy must be implemented consistent with Policy 1101. Unless ~~expressly~~ prohibited ~~by~~because of a collective bargaining agreement and to the maximum extent permitted by law, the Board or designee may contract with third parties as determined by the Board.

Any selected third-party contractor must fully comply with Policies 2202 and 4205(C).

Legal authority: MCL 380.11a(3)

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4207 Third-Party Contracting

This Policy must be implemented consistent with Policy 1101. Unless prohibited because of a collective bargaining agreement and to the maximum extent permitted by law, the Board or designee may contract with third parties as determined by the Board.

Any selected third-party contractor must fully comply with Policies 2202 and 4205(C).

Legal authority: MCL 380.11a(3)

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4209 ~~*Prohibition Against*~~ *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 or legal guardian~~Parent of that student.

~~If a parent/guardian of a student enrolled in the District believes that a District official, Board member, or District employee has violated this Policy, the parent/guardian may file a complaint with the Superintendent, who will investigate the complaint and, within 30 calendar days after the date of the complaint, provide a written report of his/her finding to the complainant and to the Superintendent of Public Instruction in accordance with state law. If a violation is substantiated, the Board or designee will discipline that person in accordance with the law, Board Policy, and any applicable collective bargaining agreement or individual employment contract. See Policy 2303. The Superintendent or designee will take corrective action to ensure that there is no further violation.~~

Legal Authority: MCL 380.~~1507; MCL 388.1766, 388.1766a~~11as

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 380.11as

Date Adopted: August 15, 2022

Date Revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4213 Anti-Nepotism

A. General

Employment decisions motivated by nepotism, as defined below, are prohibited to avoid conflicts of interest, favoritism, and lost productivity. Employment decisions will be based on qualifications, experience, and other legitimate business reasons. This Policy applies to all categories of employment including regular, temporary, and part-time classifications.

B. Definitions

1. "Nepotism" means favoritism in the workplace based on a relationship with a relative or significant other.

2. "Relative" means a spouse, child, ~~p~~Parent, sibling, grandparent, grandchild, aunt, uncle, first cousin, niece, nephew, or corresponding in-law, step, or adopted relative.

3. "Significant others" means (1) persons engaged to be married, (2) persons involved in a romantic or personal relationship, or (3) persons who are cohabitating.

C. Employment Decisions

The District may employ relatives and significant others in the absence of nepotism. In making employment decisions, including hiring, placement, supervision, directing work, promoting, compensating, evaluating, and disciplining employees who are a relative or significant other, an employee should:

1. disclose the existence of any relationships subject to this Policy to the Superintendent or designee;

2. avoid conflicts of interest, as defined in Policy 4201, and any appearance of a conflict of interest; and

3. avoid favoritism and any appearance of favoritism.

An employee's relative or significant other should not be hired to work in any position in which the Board or designee concludes a conflict of interest or the appearance of a conflict of interest may exist. Relatives and significant others are permitted to work at the District provided one does not report directly to, supervise, evaluate, or manage the other. The Superintendent ~~or designee, or the Board, as applicable,~~ may make exceptions to this Policy~~.~~ when in the District's best interest with [Option 1: Board approval] [Option 2: prompt notice to the Board].

Supervisors and subordinates who become relatives or significant others while employed may be subject to transfer, reassignment, or other action based on the need for compliance with this Policy.

Legal authority: MCL 380.11a, 380.601a

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4213 Anti-Nepotism

A. General

Employment decisions motivated by nepotism, as defined below, are prohibited to avoid conflicts of interest, favoritism, and lost productivity. Employment decisions will be based on qualifications, experience, and other legitimate business reasons. This Policy applies to all categories of employment including regular, temporary, and part-time classifications.

B. Definitions

1. "Nepotism" means favoritism in the workplace based on a relationship with a relative or significant other.

2. "Relative" means a spouse, child, Parent, sibling, grandparent, grandchild, aunt, uncle, first cousin, niece, nephew, or corresponding in-law, step, or adopted relative.

3. "Significant others" means (1) persons engaged to be married, (2) persons involved in a romantic or personal relationship, or (3) persons who are cohabitating.

C. Employment Decisions

The District may employ relatives and significant others in the absence of nepotism. In making employment decisions, including hiring, placement, supervision, directing work, promoting, compensating, evaluating, and disciplining employees who are a relative or significant other, an employee should:

1. disclose the existence of any relationships subject to this Policy to the Superintendent or designee;

2. avoid conflicts of interest, as defined in Policy 4201, and any appearance of a conflict of interest; and

3. avoid favoritism and any appearance of favoritism.

An employee's relative or significant other should not be hired to work in any position in which the Board or designee concludes a conflict of interest or the appearance of a conflict of interest may exist. Relatives and significant others are permitted to work at the District provided one does not report directly to, supervise, evaluate, or manage the other. The Superintendent may make exceptions to this Policy when in the District's best interest with Board approval.

Supervisors and subordinates who become relatives or significant others while employed may be subject to transfer, reassignment, or other action based on the need for compliance with this Policy.

Legal authority: MCL 380.11a, 380.601a

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4214 Outside Activities and Employment

A. General

An employee's duties to the District take precedence over other outside obligations while performing District duties or during work hours. An employee may not engage in other activities that adversely impact school employment or operation or that interfere with the employee's duties.

Except as otherwise provided in these Policies, an employee may secure additional employment, participate in business ventures, and serve as a volunteer. Such activities must not interfere with an employee's ability to carry out the employee's responsibilities, to serve as a role model in the community, or adversely impact the District's reputation.

Employees must communicate with a supervisor before engaging in outside activities where a conflict of interest (as defined in Policy 4201) or the appearance of a conflict of interest or impropriety may exist.

B. Conduct Standards

Employees must fulfill their duties without conflict from outside employment or activities. Unless the Superintendent or designee grants written authorization, employees may not engage in the following outside activities:

1. provide private services, lessons, tutoring, or coaching for students assigned to the employee for additional remuneration;

2. conduct personal business during assigned duty hours;

3. represent, either expressly or by implication, that the District sponsors, sanctions, or endorses a non-District related activity, solicitation, or other endeavor;

4. sell, solicit, or promote the sale of goods or services to students or ~~parents/guardians~~Parents when the employee's relationship with the District is used to influence the sale or may be reasonably perceived as attempting to influence the sale;

5. sell, solicit, or promote the sale of goods or services to employees over whom the employee has supervisory or managerial responsibilities in a manner that the subordinate employee could reasonably perceive as coercive;

6. use employee, student, or ~~parent/guardian~~Parent information in connection with the solicitation, sale, or promotion of goods or services or provide that information to any person or entity for any purpose; or

7. use District personnel, facilities, resources, equipment, technology, property, or funds for personal financial gain or business activity.

C. Intellectual Property

Intellectual property includes written or artistic works, instructional materials, textbooks, curriculum, software, inventions, procedures, ideas, innovations, systems, programs, or other work product created or developed by an employee in the course and scope of performing District employment duties or during work hours, or derivative to District intellectual property, whether published or not. Such intellectual property will be the exclusive property of the District. The District has the sole right to sell, copy, license, assign, or transfer any and all right, title, or interest in and to that intellectual property.

Legal authority: 17 USC 101 et seq.; MCL 15.321 et seq., 15.401 et seq.; MCL 380.11a, 380.601a, 380.1805(1)

Date adopted:

Date revised:

4200 Employee Conduct and Ethics

4214 Outside Activities and Employment

A. General

An employee's duties to the District take precedence over other outside obligations while performing District duties or during work hours. An employee may not engage in other activities that adversely impact school employment or operation or that interfere with the employee's duties.

Except as otherwise provided in these Policies, an employee may secure additional employment, participate in business ventures, and serve as a volunteer. Such activities must not interfere with an employee's ability to carry out the employee's responsibilities, to serve as a role model in the community, or adversely impact the District's reputation.

Employees must communicate with a supervisor before engaging in outside activities where a conflict of interest (as defined in Policy 4201) or the appearance of a conflict of interest or impropriety may exist.

B. Conduct Standards

Employees must fulfill their duties without conflict from outside employment or activities. Unless the Superintendent or designee grants written authorization, employees may not engage in the following outside activities:

1. provide private services, lessons, tutoring, or coaching for students assigned to the employee for additional remuneration;

2. conduct personal business during assigned duty hours;

3. represent, either expressly or by implication, that the District sponsors, sanctions, or endorses a non-District related activity, solicitation, or other endeavor;

4. sell, solicit, or promote the sale of goods or services to students or Parents when the employee's relationship with the District is used to influence the sale or may be reasonably perceived as attempting to influence the sale;

5. sell, solicit, or promote the sale of goods or services to employees over whom the employee has supervisory or managerial responsibilities in a manner that the subordinate employee could reasonably perceive as coercive;

6. use employee, student, or Parent information in connection with the solicitation, sale, or promotion of goods or services or provide that information to any person or entity for any purpose; or

7. use District personnel, facilities, resources, equipment, technology, property, or funds for personal financial gain or business activity.

C. Intellectual Property

Intellectual property includes written or artistic works, instructional materials, textbooks, curriculum, software, inventions, procedures, ideas, innovations, systems, programs, or other work product created or developed by an employee in the course and scope of performing District employment duties or during work hours, or derivative to District intellectual property, whether published or not. Such intellectual property will be the exclusive property of the District. The District has the sole right to sell, copy, license, assign, or transfer any and all right, title, or interest in and to that intellectual property.

Legal authority: 17 USC 101 et seq.; MCL 15.321 et seq., 15.401 et seq.; MCL 380.11a, 380.601a, 380.1805(1)

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4215 District Technology and Acceptable Use ~~Policy~~

The Board provides students, employees, volunteers, and other authorized users access to the District's technology resources, including its computers and network resources, for educational and other District purposes, in a manner that encourages responsible use. Any use of technology resources that violates federal and state law is prohibited.

Employees have no expectation of privacy when using the District's technology resources. Information and records on the District's network may be subject to disclosure under the Freedom of Information Act, and the District may monitor or access employees' electronic files, as deemed necessary.

Employees must not use District technology resources to record students, ~~parents/guardians~~Parents, or District personnel or to record a non-public meeting, unless performed for a legitimate educational purpose. The recording must be authorized by a supervisor or Policy. Unauthorized recording or dissemination of a recording may be subject to discipline, including discharge.

Employees must not use a password other than their own to access District technology resources unless authorized by a supervisor. Employees must protect their password(s) from being used by others. An employee will be responsible for any misuse if the employee failed to adequately secure their password(s).

District technology resources are provided for District-related services. Employees must minimize personal use of District technology resources and are prohibited from using those resources when doing so interferes with the employee's job responsibilities or District operations.

Requests for District records must be promptly directed to the FOIA Coordinator under Policy 3501. Only authorized employees may disclose District records to third parties unless otherwise permitted by law.

Employees must not permit students to engage in non-instructional computer games, movies, videos, and activities during the work or school day, unless authorized by a supervisor.

Employees must not download unauthorized software or applications.

Employees must immediately notify the District's technology department of any unauthorized access to, misuse of, or interference with the District's technology resources.

Employees must abide by Policy 3116 pertaining to District Technology and Acceptable Use, including complying with the Children's Internet Protection Act and executing an Acceptable Use Agreement.

Legal authority: 47 USC 254; MCL 397.606

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4215 District Technology and Acceptable Use

The Board provides students, employees, volunteers, and other authorized users access to the District's technology resources, including its computers and network resources, for educational and other District purposes, in a manner that encourages responsible use. Any use of technology resources that violates federal and state law is prohibited.

Employees have no expectation of privacy when using the District's technology resources. Information and records on the District's network may be subject to disclosure under the Freedom of Information Act, and the District may monitor or access employees' electronic files, as deemed necessary.

Employees must not use District technology resources to record students, Parents, or District personnel or to record a non-public meeting, unless performed for a legitimate educational purpose. The recording must be authorized by a supervisor or Policy. Unauthorized recording or dissemination of a recording may be subject to discipline, including discharge.

Employees must not use a password other than their own to access District technology resources unless authorized by a supervisor. Employees must protect their password(s) from being used by others. An employee will be responsible for any misuse if the employee failed to adequately secure their password(s).

District technology resources are provided for District-related services. Employees must minimize personal use of District technology resources and are prohibited from using those resources when doing so interferes with the employee's job responsibilities or District operations.

Requests for District records must be promptly directed to the FOIA Coordinator under Policy 3501. Only authorized employees may disclose District records to third parties unless otherwise permitted by law.

Employees must not permit students to engage in non-instructional computer games, movies, videos, and activities during the work or school day, unless authorized by a supervisor.

Employees must not download unauthorized software or applications.

Employees must immediately notify the District's technology department of any unauthorized access to, misuse of, or interference with the District's technology resources.

Employees must abide by Policy 3116 pertaining to District Technology and Acceptable Use, including complying with the Children's Internet Protection Act and executing an Acceptable Use Agreement.

Legal authority: 47 USC 254; MCL 397.606

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4216 Personal Communication Devices

"Personal communication devices" include employee-owned cell phones, computers, tablets, or any other device that 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 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 personal communication devices shall not interfere with instructional activities or work-related duties. Employees taking an authorized break may use personal communication 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 personal communication 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 personal communication devices to inappropriately communicate with other employees, students, and ~~parents/guardians~~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 device;

E. employees recognize that when a personal communication 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 personal communication 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~~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

4200 Employee Conduct and Ethics

4216 Personal Communication Devices

"Personal communication devices" include employee-owned cell phones, computers, tablets, or any other device that 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 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 personal communication devices shall not interfere with instructional activities or work-related duties. Employees taking an authorized break may use personal communication 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 personal communication 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 personal communication devices to inappropriately communicate with other employees, students, and 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 device;

E. employees recognize that when a personal communication 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 personal communication 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 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

Series 4000: District Employment

4200 Employee Conduct and Ethics

4217 Social Media

Employee use of social media while on District property, during work hours, or while using District-owned devices must not interfere with District educational purposes or work performance and must not be used in any manner that violates this Policy, Policy 4201, or federal or state law.

"Social media" refers to any publicly accessible internet-based service that enables a user to share communications, images, or videos with others or participate in social networking. Social media includes blogs and social networking sites.

While using social media on or off duty, an employee must:

A. not engage in criminal activity;

B. make clear that the employee's views or endorsement of political candidates and political parties are their own, not the District's, as applicable;

C. refrain from using a District email address to register on social networks, blogs, or other online tools for personal use;

D. engage in appropriate communications with students, ~~parents/guardians~~Parents, and District stakeholders and community members;

E. maintain student privacy and not disclose confidential student information;

F. report to the appropriate administrator(s) any behavior or activity which endangers student or staff security, safety, or welfare; and

G. refrain from engaging in behavior that disrupts or adversely impacts the efficacy of the District's operations.

Employee use of social media in violation of this Policy detracts from the District's educational mission, adversely impacts the District, and may result in discipline, including discharge.

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

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4217 Social Media

Employee use of social media while on District property, during work hours, or while using District-owned devices must not interfere with District educational purposes or work performance and must not be used in any manner that violates this Policy, Policy 4201, or federal or state law.

"Social media" refers to any publicly accessible internet-based service that enables a user to share communications, images, or videos with others or participate in social networking. Social media includes blogs and social networking sites.

While using social media on or off duty, an employee must:

A. not engage in criminal activity;

B. make clear that the employee's views or endorsement of political candidates and political parties are their own, not the District's, as applicable;

C. refrain from using a District email address to register on social networks, blogs, or other online tools for personal use;

D. engage in appropriate communications with students, Parents, and District stakeholders and community members;

E. maintain student privacy and not disclose confidential student information;

F. report to the appropriate administrator(s) any behavior or activity which endangers student or staff security, safety, or welfare; and

G. refrain from engaging in behavior that disrupts or adversely impacts the efficacy of the District's operations.

Employee use of social media in violation of this Policy detracts from the District's educational mission, adversely impacts the District, 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

4200 Employee Conduct and Ethics

4221 Employee Speech

As role models, employees must exercise sound judgment in their interactions with students, ~~parents/guardians~~Parents, and members of the community and maintain a high degree of professionalism and objectivity. Employees must act within the scope of their respective duties and responsibilities.

A. Curriculum, Instruction, and Controversial Topics

During instruction and discussion of controversial issues, employees must follow these guidelines:

1. the issues discussed must be relevant to the curriculum and be part of a planned educational program;
2. students and ~~parents/guardians~~Parents must have free access to appropriate materials and information for analysis and evaluation of the issues;
3. employees must allow discussion of a variety of viewpoints so long as that discussion does not substantially disrupt the educational environment;
4. the topic and materials used must be within the students' range, knowledge, maturity, and competence;
5. employees must obtain pre-approval from the building principal before instructing students about sensitive or controversial issues; and
6. employees must not advocate partisan causes, sectarian religious views, or self-propaganda of any kind during school or school-related functions. Employees may express a personal opinion as long as students are encouraged to reach independent decisions.

Employees who are unsure of their obligations must confer with their building principal or supervisor.

B. Speech on Matters of Public Concern

The District respects and supports its employees' right as citizens to exercise free speech in a responsible manner.

Free speech rights are not absolute and are subject to restriction when the employee is acting within the course and scope of their employment.

When speaking as a citizen on a matter of public concern, an employee must not make written, verbal, online, or nonverbal statements that cause a substantial disruption to the school environment, violate federal or state law, or otherwise violate these Policies. An employee's right as a citizen to comment upon matters

of public concern must be balanced against the District's interest in promoting the efficiency of the public services it performs through its employees.

Employees do not speak on behalf of the District or a school unless specifically authorized by the Board or Superintendent.

Legal authority: U.S. CONST. amend. I; Const 1963, art I, § 5

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4221 Employee Speech

As role models, employees must exercise sound judgment in their interactions with students, Parents, and members of the community and maintain a high degree of professionalism and objectivity. Employees must act within the scope of their respective duties and responsibilities.

A. Curriculum, Instruction, and Controversial Topics

During instruction and discussion of controversial issues, employees must follow these guidelines:

1. the issues discussed must be relevant to the curriculum and be part of a planned educational program;
2. students and Parents must have free access to appropriate materials and information for analysis and evaluation of the issues;
3. employees must allow discussion of a variety of viewpoints so long as that discussion does not substantially disrupt the educational environment;
4. the topic and materials used must be within the students' range, knowledge, maturity, and competence;
5. employees must obtain pre-approval from the building principal before instructing students about sensitive or controversial issues; and
6. employees must not advocate partisan causes, sectarian religious views, or self-propaganda of any kind during school or school-related functions. Employees may express a personal opinion as long as students are encouraged to reach independent decisions.

Employees who are unsure of their obligations must confer with their building principal or supervisor.

B. Speech on Matters of Public Concern

The District respects and supports its employees' right as citizens to exercise free speech in a responsible manner.

Free speech rights are not absolute and are subject to restriction when the employee is acting within the course and scope of their employment.

When speaking as a citizen on a matter of public concern, an employee must not make written, verbal, online, or nonverbal statements that cause a substantial disruption to the school environment, violate federal or state law, or otherwise violate these Policies. An employee's right as a citizen to comment upon matters

of public concern must be balanced against the District's interest in promoting the efficiency of the public services it performs through its employees.

Employees do not speak on behalf of the District or a school unless specifically authorized by the Board or Superintendent.

Legal authority: U.S. CONST. amend. I; Const 1963, art I, § 5

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4228 No Expectation of Privacy

Employees have no expectation of privacy in connection with their use of District property and equipment. The District reserves the right to search District property, equipment, and technology issued or provided for the employee's use during the employee's District employment, including but not limited to the employee's office, desk, files, computer, or locker. Inspections may be conducted at any time at the District's discretion. A search of an employee's personal effects will comply with federal and state constitutional protections, laws, and regulations.

Legal Authority: U.S. Const, amend. IV

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4228 No Expectation of Privacy

Employees have no expectation of privacy in connection with their use of District property and equipment. The District reserves the right to search District property, equipment, and technology issued or provided for the employee's use during the employee's District employment, including but not limited to the employee's office, desk, files, computer, or locker. Inspections may be conducted at any time at the District's discretion. A search of an employee's personal effects will comply with federal and state constitutional protections, laws, and regulations.

Legal Authority: U.S. Const, amend. IV

Date adopted: August 15, 2022

Date revised: August 19, 2024

Series 4000: District Employment

4200 Employee Conduct and Ethics

4229 Acceptable Use of Generative Artificial Intelligence [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.]

Employees may use Generative Artificial Intelligence ("Generative AI") in the school setting in compliance with this Policy and applicable law.

A. Definitions

1. "Generative AI" means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This may include images, videos, audio, text, and other digital content.

2. "AI System" means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

B. Acceptable Use

Employee use of Generative AI must be appropriate for the educational environment and in compliance with all applicable laws, including, but not limited to, the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the Children's Internet Protection Act. Employees must also comply with applicable Board Policies when using Generative AI, including, but not limited to, policies on District technology and acceptable use, copyright protection, student records, unlawful harassment, discrimination, and employee ethics.

[Optional: Employees must obtain prior approval from the Superintendent or designee before using Generative AI Systems for District-related purposes.]

Employees must thoroughly review AI-generated material to ensure accuracy, relevance, and appropriateness. Employees may not rely solely on Generative AI to deliver instructional or work-related material. Employee use of Generative AI in the classroom must align with the Board-approved curriculum.

C. Training

Employees may receive training on the legal and ethical use of Generative AI and its integration into the curriculum.

D. Violations

Violations of this policy may result in disciplinary action, up to and including discharge.

Legal Authority: 20 USC 1232g; 20 USC 1400 et seq.; 34 CFR 99; 47 CFR 54.520; 88 Fed Reg 75191 (October 30, 2023)

Date adopted:

Date revised:

Series 4000: District Employment

4200 Employee Conduct and Ethics

4229 Acceptable Use of Generative Artificial Intelligence

Employees may use Generative Artificial Intelligence ("Generative AI") in the school setting in compliance with this Policy and applicable law.

A. Definitions

1. "Generative AI" means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This may include images, videos, audio, text, and other digital content.

2. "AI System" means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

B. Acceptable Use

Employee use of Generative AI must be appropriate for the educational environment and in compliance with all applicable laws, including, but not limited to, the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the Children's Internet Protection Act. Employees must also comply with applicable Board Policies when using Generative AI, including, but not limited to, policies on District technology and acceptable use, copyright protection, student records, unlawful harassment, discrimination, and employee ethics.

Employees must thoroughly review AI-generated material to ensure accuracy, relevance, and appropriateness. Employees may not rely solely on Generative AI to deliver instructional or work-related material. Employee use of Generative AI in the classroom must align with the Board-approved curriculum.

C. Training

Employees may receive training on the legal and ethical use of Generative AI and its integration into the curriculum.

D. Violations

Violations of this policy may result in disciplinary action, up to and including discharge.

Legal Authority: 20 USC 1232g; 20 USC 1400 et seq.; 34 CFR 99; 47 CFR 54.520; 88 Fed Reg 75191 (October 30, 2023)

Date adopted: August 19, 2024

Date revised: