MOBILE COUNTY PUBLIC SCHOOL SYSTEM POLICY BOOK

CHAPTER 3: GENERAL ADMINISTRATION

Chapter 3.00 – General Administration

3.10 Superintendent Selection / Contract
3.11 Superintendent Duties
3.12 Board-Superintendent Relations

3.20 Administrative Rules

3.30 Equal Opportunity
3.31 Title IX
Section IX - Sexual Harassment
3.32 Website Accessibility
3.33 Service Animals

3.40 Safety
3.41 Tobacco Use
3.42 Firearm Possession

3.50 Computer, Internet and Electronic Communication Acceptable Use
3.51 Copyright
3.52 Professional Publishing
3.53 Data Use and Governance

3.60 School Volunteers
3.61 Fundraising
3.62 Associations/Collectives

3.70 School Facility Use

3.80 Flag Displays

SUPERINTENDENT SELECTION / CONTRACT

The board will appoint the superintendent based on its qualifications and state requirements and will negotiate an employment contract addressing compensation, benefits outside those established by state law, expense allowance, professional development, consulting contracts and evaluation (outside of that required by state Board of Education) discharge and resignation.

Legal Reference: Alabama Code - §16-9-9; §16-9-10; §16-9-12; §16-13A-3
Date Adopted: December 11, 2007

SUPERINTENDENT DUTIES

The duties of the superintendent are:

1. He/she shall provide leadership in working with the Board of School Commissioners of Mobile County, professional associates, and citizens generally in formulating educational objectives for the schools, which are based on community needs and students' abilities and needs.

2. He/she shall serve as the executive officer of the board; and shall sign in the name of the board all deeds, bills of sale, contracts or evidence of debt, and other legal documents to which the board is a party except such, as by other resolution or action, are to be signed by the president or other officers or employee of the board.

3. He/she shall give general direction, supervision, and coordinated leadership to the entire school program, including business administration, curriculum development and instruction, personnel administration, pupil personnel administration, and all auxiliary services associated with the operation of public schools.

4. He/she shall understand laws and court decisions bearing upon education and policies, both of the State Board of Education and of the Board of School Commissioners of Mobile County, and shall administer the schools of Mobile County in accordance with same, insofar as they may be applicable to Mobile County.

5. He/she shall develop administrative procedures that will achieve effective implementation of school board objectives and policies.

6. He/she shall implement procedures designed to attract capable and properly trained personnel to specialized jobs necessary to the operation of schools; shall promote in-service growth and improvement of all workers on their jobs; shall foster esprit de corps, high morale, and teamwork among the board's employees and the best possible utilization of specialized abilities and interests.

7. He/she shall assist the board in carrying out its functions by providing channels of communication between the board and the educational community, the administrative staff, and lay citizens.

8. He/she shall promote a continuous program of research in all phases of the school program; shall facilitate an effective evaluation of the program in terms of the objectives sought; shall furnish information needed by the board in policy formation, in making important decisions, in improving administration, and in achieving economical and wise business administration.

9. He/she shall serve the board as secretary, conduct all correspondence of the board, keep and preserve all of its records, receive all reports required by the board and ascertain that all reports are in proper form, complete and accurate, arrange and announce meetings, prepare agendas for meetings, attend all meetings unless otherwise excused by the board president, participate in all deliberations other than those involving his/her salary and employment, and prepare minutes of meetings for school board approval.

10. He/she shall recommend professional employees for appointment, demotion, promotion, transfer, or dismissal.

11. He/she shall give leadership in a continuous program of curriculum development so the instructional program will be adapted to the needs of the community, the larger society, and to the needs and abilities of students.

12. He/she shall prepare and submit to the board before the end of the fiscal year an estimate of receipts and expenditures for the ensuing year.

13. He/she shall organize the central staff in such a way as to accomplish the following:
    a. Teamwork through cooperative planning.
    b. Clarification of purposes to be achieved.
    c. Understanding of basic policies and administrative procedures designed for their implementation.
    d. Effective utilization of specialized interests, abilities, and training.
    e. Clear understanding of duties and responsibilities to be performed.
    f. Creation of an emotional and professional climate conducive to a realistic, objective, and rational approach to solving problems.
    g. Performing such other duties as the board may determine.

Legal Reference: See generally Code of Alabama (Chapter 9 of Title 16).
Date Adopted: December 11, 2007

BOARD-SUPERINTENDENT RELATIONS

The superintendent represents the board in dealing with the staff; he or she likewise represents the staff in dealing with the board. Board members who have information or suggestions pertinent to the administration of schools call or contact the superintendent. Staff members who desire advice and counsel or clarification of policy in handling complicated problems contact the superintendent, who in turn gives the answer or direction needed or else seeks the assistance of the board. Staff members who have information or suggestions pertinent to the carrying out of school board functions bring them to the attention of the superintendent who in turn makes regular reports to the board.

Board members will refer all requests for individual adjustment, preferment, or promotion to the superintendent.

The board and the superintendent will respect the confidentiality of personal information pending school board action and/or the resolution of problems, to a satisfactory conclusion in a confidential and professional manner.

Board members desiring written response and/or research by staff members should present such requests to the superintendent or designee in writing.

Copies of the written board requests and staff responses shall be disseminated to all board members and appropriate staff members through the superintendents or designee.

Date Adopted: December 11, 2007

ADMINISTRATIVE RULES

Following the adoption of policies governing the operation of the school system, the superintendent and administrative staff will develop procedures for the implementation throughout the system.

Legal Reference: Alabama Code - §16-9-13
Date Adopted: December 11, 2007

EQUAL OPPORTUNITY

The board, its employees and agents shall not discriminate in any way on the basis of race, sex, religion, national origin, age or handicap.

Guidelines will be maintained to support nondiscrimination. These guidelines specify grievance procedures, including the name and location of the board employee(s) assigned responsibility for grievances.

Equal Opportunity: Complaints, Appeals

Any student, parent or other individual on behalf of a student or parent may file a written complaint or appeal for an exception to any school board practice. Administrative procedures for reviewing all complaints will be designed to secure solutions at the lowest level.

All complaints will be handled promptly as soon as possible and resolved within 30 days after the complaint is filed unless additional time is required because of exceptional circumstances.

Reference – Procedures: Equal Opportunity, Complaints, Appeals

Date Adopted: December 11, 2007

PROCEDURE:
EQUAL OPPORTUNITY, COMPLAINTS, APPEALS FOR NON EMPLOYEES

Normal steps in reaching a resolution to individual concerns are listed below:

1. In the event an individual or group believes there is a basis for complaint, that person or group will initiate informal discussion within 5 days after he/she knew, or should have known of the occurrence leading to the possible concern.

2. If the complaint is not resolved at the informal level, the complainant may FILE a written complaint and supporting evidence with the superintendent or his specified designee.

3. Within ten days, the superintendent's designee will discuss the matter with the complainant; thereafter a thorough investigation will be conducted to gather all relevant information. Equal rights for discussion will be given to other appropriate parties.

4. If the complaint is not settled through the discussion process the superintendent may designate a hearing officer, and a formal hearing will be scheduled to permit both parties to present evidence before the hearing officer.

5. If satisfaction is not reached with the hearing officer's formal recommendations, the grievant may request a hearing before the school board.

Title IX

A. Prohibition - In accordance with Title IX (20 U.S.C. §1681, *et seq*.), and its regulations (34 C.F.R. Part 106), the Board strictly prohibits discrimination on the basis of sex or gender in its programs or activities, including sexual harassment, as defined by law and Board policy. Inquiries regarding the application of Title IX regulations may be referred to the Board's Title IX Coordinator, to the Assistant Secretary for Civil Rights of the Department of Education, or both. Sexual harassment complaints will be filed and reviewed under the Board's student sexual harassment policy or its employee sexual harassment policy as applicable. All other complaints under Title IX will be filed and reviewed according to the Board's general complaint and grievance procedures.

B. Title IX Coordinator - The Superintendent has designated a Title IX Coordinator, whose duties will include but not be limited to receiving and responding to Title IX inquiries and complaints, and compliance with the regulations. The Title IX Coordinator is Bryan Hack, Human Resources Supervisor, 1 Magnum Pass, P.O. Box 180069, Mobile, AL 36618 (251) 221-4543, Bhack@mcpss.com.

C. Reports to State Department of Human Resources - When alleged sexual harassment involves a student and could involve sexual abuse, certified personnel must report it to the state Department of Human Resources as required under Alabama law.

Legal References: 20 U.S.C. §1681, *et seq.*; 34 C.F.R. Part 106; Ala. Code §26-14.3
Revised: _____

SECTION IX

SEXUAL HARASSMENT

The Board does not discriminate on the basis of sex in its education programs or activities it operates, nor does it tolerate sexual harassment. All inquiries, questions, or comments regarding Title IX concerns should be sent to: Bryan Hack, Human Resources Supervisor, Title IX Coordinator, 1 Magnum Pass, P.O. Box 180069, Mobile, AL 36618 (251) 221-4543, Bhack@mcpss.com. In accordance with Board Policy 5.281, all complaints regarding *sexual harassment* should be filed and reviewed under the Board's student sexual harassment policy and procedures. The procedures are set forth below. Any person may report sex discrimination, including sexual harassment (whether or not the person reporting is the person alleged to be the victim of conduct that could constitute sex discrimination or sexual harassment), in person, by mail, by telephone, or by electronic mail, using the contact information listed for the Title IX Coordinator receiving the person's verbal or written report. All other complaints under Title IX should be filed with the Title IX Coordinator and will be reviewed according to the Board's general complaint and grievance policy and procedures.

Sexual harassment, as defined in the Board Policy 5.281 and herein, in any form that is directed toward students is prohibited. Persons who violate the policy will be subject to the full range of disciplinary consequences, up to and including termination (for employees), and expulsion (for students) as dictated by the nature and severity of the violation and other relevant considerations. If appropriate, the circumstances constituting the violation may be reported to law enforcement agencies or child welfare agencies for further investigation and action. The Board reserves the right to modify these policies and procedures in order to comply with applicable law. In the event that any court, agency, commission, legislative body, or other authority of competent jurisdiction issues a finding that limits the validity or enforceability of Title IX or its implementing regulations, in whole or in part, the Board's policies and procedures shall be deemed modified and/or limited to the extent necessary to comply with any applicable court, agency, commission, legislative body, or other authority's finding or order.

A. Definitions -

1. Complainant - complainant means a student who is alleged to be the victim of conduct that could constitute sexual harassment.

2. Respondent - respondent means and individual who has been reported to be the perpetrator of conduct that could constitute sexual harassment.

3. Sexual harassment - For purposes of the Title IX sexual harassment policies and procedures, sexual harassment means conduct on the basis of sex that satisfies one or more of the following:

a. Sexual assault as defined in 20 U.S.C. §1092(f)(6)(A)(v), dating violence as defined in the 34 U.S.C. §12291(a)(10), domestic violence as defined in 34 U.S.C. §12991(a)(8), or stalking as defined in 34 U.S.C. §12291(a)(30).

b. Unwelcome conduct determined by a reasonable person to be so severe, pervasive, and objectively offensive that it effectively denies a person equal access to the recipient's education program or activity: or

c. An employee of the Board conditioning the provision of an aid, benefit or service of the Board on and individual's participation in unwelcome sexual conduct (otherwise known as "quid pro quo").

4. Formal Complaint - Formal complaint means a document filed by a complainant or signed by the Title IX Coordinator alleging sexual harassment against a respondent and requesting that the school system investigate the allegation of sexual harassment. At the time of filing a formal complaint, a complainant must be participating in or attempting to participate in the education program or activity in the school system for which the complaint relates to.

5. Actual knowledge - Actual knowledge means notice of sexual harassment or allegations of sexual harassment to: (1) the Title IX Coordinator, (2) any official of the school system who has authority to institute corrective measures on behalf of the school system, or (3) to any other employee of the Mobile County Public School System. This standard is not met when the only official of the school system with actual knowledge is the respondent (alleged perpetrator).

6. Supportive Measures - Supportive Measures means non-disciplinary, non-punitive, individualized services offered as appropriate, as reasonably available, and without fee or charge to the complainant or the respondent before or after the filing of a formal complaint, and/or where no formal complaint has been filed. Such measures are designed to restore or preserve equal access to the school system's education program or activity without unreasonably burdening the other party, including measures designed to protect the safety of all parties or the school system's educational environment, or deter sexual harassment. Supportive measures may include, but not be limited to:

a. counseling

b. extensions of deadlines or other course-related adjustments;

c. modifications of work or class schedules;

d. campus escort services;

e. mutual restrictions on contact between the parties;

f. changes or modifications to student schedules;

g. increased security and monitoring of certain areas of campus; and

h. other similar measures.

7. Education program or activity - "Education program or activity" includes locations, events, or circumstances over which the Board exercises substantial control over both the respondent and the context in which the sexual harassment occurs.

B. Jurisdictional issues

An administrator, campus principal, or his or her designee, may address student issues and impose discipline and/or sanctions through a separate Student Code of Conduct provision if any student acts are found to fall outside the jurisdiction of the Board's sexual harassment policy: In accordance with Title IX's implementing regulations, the following are outside the jurisdiction and scope of the sexual harassment policy:

1. **Outside educational program.** Alleged behavior that occurs off-campus, outside an educational activity or program, and only has an on-campus effect;
2. **Outside the United States.** Alleged behavior that occurs outside the United States.
3. **Outside definition of Sexual Harassment.** Alleged behavior that falls outside the definition of "sexual harassment."

C. Presumption under Title IX

Under Title IX and its implementing regulations, it is presumed that the respondent is not responsible for the alleged conduct until a determination regarding responsibility is made at the conclusion of the grievance process.

D. Informal Report of Sexual harassment and Response

1. Report - In accordance with Title IX of the Education Amendments of 1972, and its implementing regulations, found at 34 C.F.R. § 106.44(a), any person may report sex discrimination, including sexual harassment, (whether or not the person reporting is the person alleged to be the victim of conduct that could constitute sex discrimination or sexual harassment), in person, by mail, by telephone, or by electronic mail, using the contact information listed for the Title IX Coordinator as identified in this Code of Conduct, or by any other means that results in the Title IX Coordinator receiving the person's verbal or written report. Such a report may be made at any time, by using the telephone number or email address, or by mail to the office address listed for the Title IX Coordinator above.

Students are also permitted to report allegations of suspected sex discrimination, including sexual harassment to any other administrator, teacher, counselor, or any other Board employee. All Board employees have a duty to promptly refer such allegations to the building principal, so long as the building principal is not the Respondent and/or not alleged to be involved with the report of sexual harassment, and/or the Title IX Coordinator, or his or her designee. If the report involves the campus principal, the report shall be made or filed directly with the Title IX Coordinator by the reporting party or complainant. If a Board employee fails to forward any sexual harassment report or complaint as provided herein, such failure may result in disciplinary action against the Board employee.

Upon receipt of any informal report of sexual harassment from any complainant and/or Board employee, the principal should also notify the Title IX Coordinator of the report. The Title IX Coordinator will make a determination as to whether the principal should review and investigate the concerns, and/or whether the Title IX Coordinator, or his or her designee will review and investigate.

2. **Supportive Measures -** Upon receiving a informal report, or a copy of a report of sexual harassment, the Title IX Coordinator, or his or her designee, should promptly contact the complainant to discuss the availability of supportive measures, consider the complainant's wishes

with respect to supportive measures, inform the complainant of the availability of supportive measures with or without filing of a formal complaint, and explain the process of filing a formal complaint.

3. Response - Upon receiving an informal report of sexual harassment, the principal, Title IX Coordinator, or his or her designee, should respond promptly and in a manner that is not deliberately indifferent. A deliberately indifferent response is a response that is clearly unreasonable in light of known circumstances. The principal, Title IX Coordinator, or his or her designee should take steps to investigate the allegations using various procedures and investigating techniques, including but not limited to interviews, phone contact, data reviews, and witness reports.

4. Determination - Following a review and investigation of the allegations, the principal, Title IX Coordinator, or his or her designee should make a determination of whether the allegations have been substantiated as factual based on the preponderance of the evidence and whether the actions appear to be violations of this policy. If the allegations are determined to be true, and a finding is made that the Respondent engaged in sexual harassment, supportive measures may also be offered to the Respondent. In addition, if Respondent is found to have engaged in sexual harassment, responsive actions or recommendations may include any sanctions as listed in the Student Code of Conduct. *Before the imposition of any disciplinary sanctions or other actions that are not supportive measures against a respondent can be imposed, however, the formal complaint and grievance process outlined below must be initiated and followed.*

E. Formal Complaint and Grievance Process

All formal complaints of sexual harassment should comply with the requirements of 34 C.F.R. § 106.45. The formal complaint process should be investigated and findings made with reasonable promptness. Temporary delays of any of the grievance processes, and/or limited extensions of time frames, will be allowed for (1) good cause, with (2) written notice to the complainant and the respondent of the delay or extension, and (3) the reasons for such action. Good cause may include but not be limited to, considerations such as the absence of a party, a party's advisor, a witness, concurrent law enforcement activity, or the need for language assistance or accommodation of disabilities.

In accordance with the requirements of 34 C.F.R. § 106.45, the following procedures will apply to the formal complaint process.

1. Filing the Formal Complaint

A complainant or the Title IX Coordinator may file a formal complaint of sexual harassment. Such complaints should be submitted on the Board's "Sexual Harassment Complaint Form." (attached) A complainant may file a formal complaint with the Title IX Coordinator in person, by mail, or by electronic mail, by using the contact information listed herein. The complainant should sign the document or provide their name if submitting the Sexual Harassment Complaint Form by e-mail. Where the Title IX Coordinator signs a formal complaint, the Title IX Coordinator is not a complainant or otherwise a party under 34 C.F.R. part 106 or under 34 C.F.R. § 106.45 See 34 C.F.R. § 106.30(a).

2. Notice.

Upon receipt of a formal complaint, the Title IX Coordinator, or his or her designee, shall provide written notice to the parties (complainant and respondent). The Written notice shall contain the following:

a. Notice of the Board's grievance process as outlined below, including any available informal resolution process;

b. Notice of the allegations of sexual harassment potentially constituting sexual harassment as defined and including sufficient details known at the time. Sufficient details should include the identities of the parties involved in the incident, if known, the conduct allegedly constituting sexual harassment, and the date and location of the alleged incident, if known.

c. A statement that the respondent is presumed not responsible for the alleged conduct and that a determination regarding responsibility is made at the conclusion of the grievance process.

d. A statement informing the parties that they may have an advisor, of their choice, who may be, but is not required to be, an attorney.

e. A statement informing the parties that they may inspect and review evidence gathered as a result of the formal complaint process.

f. A statement informing the parties that the Board's sexual harassment policies and procedures prohibit knowingly making false statements or knowingly submitting false information during the grievance process.

3. Dismissal of Formal complaint.

A formal complaint shall, or may, be dismissed in the following situations:

a. Mandatory Dismissal. If the conduct alleged in the formal complaint (1) would not constitute sexual harassment even if proved, (2) did not occur in the Board's education program or activity, or (3) did not occur against a person in the United States, then the Title IX Coordinator, or his or her designee, must dismiss the formal complaint with regard to that conduct for purposes of sexual harassment under Title IX. Such a dismissal does not preclude action against the respondent under another provision of the Student Code of Conduct.

b. Permissive Dismissal. The Title IX Coordinator may dismiss a formal complaint, or any allegations therein, if at any time during the investigation or grievance process:

i. The respondent is no longer enrolled in the school system and/or the respondent is no longer employed by the school system; or

ii. A complainant notifies the Title IX Coordinator in writing that the complainant would like to withdraw the formal complaint or any allegations therein;

iii. Certain circumstances prevent the Title IX Coordinator, or his or her designee, from gathering evidence sufficient to reach a

determination as to the formal complaint or allegations therein (e.g., passage of time, lack of cooperation by the complainant).

c. Written notice of dismissal. Upon a required and/or permitted dismissal pursuant to the above paragraphs of this section, the Title IX Coordinator, or his or her designee, must promptly send written notice of the dismissal and reason(s) therefore simultaneously to the parties.

4. Investigation process and Written Report.

By authority of the Board, the Title IX Coordinator, or his or her designee, upon receipt of an formal complaint alleging sexual harassment, shall promptly undertake or authorize an investigation (individual investigating is hereinafter "the appointed investigator"). The Title IX Coordinator may be the appointed investigator, or the Title IX Coordinator may choose to have the principal serve as the appointed investigator, so long as the principal is not the alleged respondent and/or so long as the formal complaint does not involve the principal. The appointed investigator may also be another Board official, or a third party as deemed appropriate under the circumstances. The appointed investigator shall conduct a formal investigation to discover and examine the facts related to the allegation(s).

The investigation process should be conducted in accordance with 34 C.F.R. 106.45(b)(5). During the investigation, the Complainant and the Respondent will have an equal opportunity to submit information and corroborating evidence, to identify witnesses who may have relevant information, and to submit questions to be asked of the other party. Questions for the other party will be asked by and at the discretion of the appointed investigator. The appointed investigator will meet separately with the complainant, the respondent, and any witnesses, and will gather other relevant and available evidence and information. To the extent possible, the investigation will be conducted in a manner that protects the privacy of all parties involved. While the Board cannot guarantee complete privacy, information collected during the investigation will be communicated only to the parties and those with a need to know in order to fulfill the purposes of Board's policies and to comply with applicable laws.

5. Written Report.

The investigation should be completed as soon as practicable. The appointed investigator should prepare a written report which fairly summarizes the relevant evidence. The appointed investigator may draw conclusions as to whether, based on the preponderance of the evidence, an allegation is substantiated, unsubstantiated, or that there is insufficient information to substantiate. The appointed investigator may also draw conclusions as to whether or not any other Student Code of Conduct provisions or policies were violated. To the extent allowed by laws that apply to matters of confidentiality, the written investigative report should be provided to the parties and their advisors in draft form prior to the appointed investigator supplying the final investigative report to the designated administrator who will make the determination of responsibility. The draft investigation report should be redacted in accordance with state and/or federal law (e.g. FERPA) before the parties' review.

After the Title IX Coordinator, or his or her appointed investigator, has sent the complainant and respondent the draft investigative report, the complainant and respondent

will have ten (10) days to prepare a written response to the draft report. The appointed investigator will consider the response(s) provided, if any, prior to completing the investigation report. The complainant and respondent's response should also contain any written, relevant questions that a party wants asked of any party or witness. Each party will then have an opportunity to provide answers, and an opportunity for any additional, limited, follow-up questions from each party. Questions and evidence about the complainant's sexual predisposition or prior sexual behavior are not relevant, unless such questions and evidence concern specific incidents of the complainant's prior sexual behavior with respect to the respondent and are offered to prove consent. The appointed investigator should inform the party proposing questions regarding any decision to exclude a question as not relevant. Ultimately, the appointed investigator has the sole discretion to determine the relevance of evidence, and whether it should be included in, or excluded, from the investigation report. Once the investigative report is complete, the appointed investigator should send the complainant and respondent a written copy of the Final Investigation Report. Both parties will be provided ten (10) days to review the Final Investigation Report and provide a written response if they desire. The Final Investigation Report will be redacted in accordance with state and/or federal law (e.g. FERPA) before the parties' review. The appointed investigator shall then submit the written report, and any responses thereto, to the designated administrator.

6. Determination regarding responsibility.

The Superintendent's designee shall be responsible for making a determination regarding responsibility, (hereinafter referred to as the "designated administrator"). The designated administrator, however, cannot be the same person as the Title IX Coordinator or the Title IX Coordinator's appointed investigator. The designated administrator must issue a written determination regarding responsibility. The Respondent is presumed to not have engaged in prohibited conduct until the designated administrator finds that there is sufficient evidence based on a preponderance of the evidence that the respondent has violated the Board's sexual harassment policy.

The designated administrator should review the investigation report, the documentary evidence, and any other relevant information to render a written decision based on the preponderance of the evidence as to 1) whether the conduct alleged occurred; and 2) whether each allegation has been substantiated, unsubstantiated, or that there is insufficient information to substantiate that respondent violated the Board's sexual harassment policy. The designated administrator may also render a written decision as to whether other provisions of the Student Code of Conduct, policies, and/or rules were violated. If violation(s) are found, the designated administrator may issue and/or recommend sanctions to the appropriate campus principal. The designated administrator should not render a written determination until both parties have been provided ten (10) days to review the above Final investigation report.

Both parties should then be provided a copy of the written determination. The written determination will be redacted in accordance with state and/or federal law before the parties' review. The written determination must include:

a. identification of the allegations potentially constituting sexual harassment;

b. a description of the procedural steps taken from the receipt of the formal complaint through the determination;

c. findings of fact supporting the determination;

d. conclusions regarding the application of the Board's Student Code of Conduct to the facts;

e. A statement of, and rationale for, the result as to each allegation, including a determination regarding responsibility, any disciplinary sanctions the designated administrator recommends being imposed on the respondent, and whether remedies designed to restore or preserve equal access to the education program or activity will be provided by the school system to the complainant; and

f. The procedures and permissible bases for the complainant and respondent to appeal.

The determination regarding responsibility becomes final either (1) on the date that the school system provides the parties with the written determination of the result of the appeal, if an appeal is filed, or (2) if an appeal is not filed, the date on which an appeal would no longer be considered timely.

A decision by the designated administrator regarding a determination of responsibility does not constitute an employment action with respect to respondent employee(s). Any sanction imposed on an employee as a result of the determination of responsibility shall be done in accordance with Board Policy and applicable state and federal law.

Any recommended sanction(s) imposed on a student respondent shall be done in accordance with the Student Code of Conduct.

7. Appeals.

a. Right to an appeal.

Should the complainant or the respondent disagree with the designated administrator's finding of responsibility and/or disagree with the Title IX Coordinator's, or his or her designee's, dismissal of a formal complaint or any allegations therein, such party shall submit a written notice of appeal within five (5) days of receiving the written determination of responsibility or dismissal of the formal complaint. The written notice of appeal should include a statement outlining the bases for appeal and any evidence which supports the appeal. The following reasons are those in which a party may appeal:

i. A procedural irregularity affected the outcome of the matter;

ii. New evidence was not reasonably available at the time the determination regarding responsibility or dismissal was made, and such evidence could affect the outcome of the matter; or

iii. The Title IX Coordinator, appointed investigator(s), or designated administrator had a conflict of interest or bias for or against complainants or respondents generally, or the individual

complainant or respondent specifically, that affected the outcome of the matter.

b. Appeal process.:

i. Upon receiving the written notice of appeal, as soon as practicable, the Title IX Coordinator, must notify the other party in writing when an appeal is filed;

ii. After receiving the notice of appeal from the Title IX Coordinator, each party will be provided five (5) days to submit a written statement in support of, or challenging, the determination.

iii. The Superintendent, or his or her designee, will hear appeals of decisions based on student-on-student sexual harassment. (appeal authority)

iv. The Superintendent will hear appeals of decisions based upon actions by Board employees. (appeal authority)

v. If (1) no appeal is filed within five (5) days of the receipt of the notice of the designated administrator's written determination; or, 2) if the appeal authority determines that the appeal does not identify one of the bases for appeal listed above, then the appeal authority will provide simultaneous notice to the parties that no valid appeal was filed and that the decision of the designated administrator is final and the case is closed.

vi. Upon receiving the notice of appeal, the Title IX Coordinator will forward the appeal, and any supporting information or evidence, to the appropriate appeal authority. The appeal authority will review the appeal documents, the written determination of responsibility by the designated administrator, any new evidence submitted by the parties, and the investigation report and exhibits. The appeal authority will render a written decision which includes a rationale for the decision as to each of the grounds appealed. The appeal authority will forward the decision to Title IX Coordinator within fourteen (14) days from the date of receipt of the appeal, unless circumstances require additional time. The decision of the appeal authority will be final.

F. Informal Resolution

The Board does not require, as a condition of enrollment, continuing enrollment, and/or enjoyment of any other right, that a complainant or respondent waive his or her right to an investigation and/or adjudication of formal complaints of sexual harassment consistent with this section. Similarly, the Board does not require the parties participate in an informal resolution process under this section, and the Board will not offer an informal resolution process unless a formal complaint is filed. However, if at any time prior to reaching a determination regarding responsibility under the **formal complaint** process, the Board reserves the right to facilitate an informal resolution process, such as mediation, that does not involve a full investigation and adjudication. Should the Title IX

Coordinator, or his or her designee, believe that an informal resolution process may be appropriate, the Title IX Coordinator, or his or her designee, shall:

1. Notice.

Provide to the parties a written notice disclosing:

i. the allegations;

ii. the requirements of the informal resolution process including the circumstances under which it precludes the parties from resuming a formal complaint arising from the same allegations;

iii. provided, however, that at any time prior to agreeing to a resolution, any party has the right to withdraw from the informal resolution process and resume the grievance process with respect to the formal complaint; and

iv. any consequences resulting from participating in the informal resolution process, including the records that will be maintained or could be shared; and

2. **Consent.**

Obtain the parties' voluntary, written consent to the informal resolution process;

3. **Student-on-Student Harassment.**

The informal resolution process will only be utilized in student-on-student complaints, and it will not be utilized to resolve allegations that an employee sexually harassed a student.

G. Confidentiality

All Board employees must keep confidential the identity of a person who complains or reports sexual harassment, including parties and witnesses, except as permitted by law and to carry out the purpose of these procedures.

Board employees should also work to maintain the confidentiality of supportive measures that are provided to the complainant or respondent, to the extent that maintaining such confidentiality would not impair the ability of the school to provide the supportive measures.

H. No Retaliation

The Board will discipline or take appropriate action against any student, teacher, administrator or other school personnel who retaliates against any person who reports sexual discrimination-including sexual harassment or violence- or any person who assists or participates in an investigation, or who assists or participates in the formal grievance process relating to such harassment or violence.

Retaliation includes, but is not limited to, any form of intimidation, reprisal or harassment. The exercise of rights protected under the First Amendment does not constitute retaliation prohibited under this section. Charging an individual with a Student Code of Conduct violation for making a materially false statement in bad faith in the course of the complaint procedure section under this part does not constitute retaliation prohibited under this section, provided, however, that a negative

determination regarding responsibility, alone, is not sufficient to conclude that any party made a materially false statement in bad faith.

I. Harassment or Violence as Abuse

Under certain circumstances, alleged harassment or violence may also be possible abuse under Alabama Law. If so, duties of mandatory reporting under Ala. Code §16-1-24 and Ala. Code §26-14-1 may be applicable.

J. Emergency removal/administrative leave

In addition to offering supportive measures to the complainant, the school system may need to initiate an emergency removal of the respondent from campus. In accordance with 34 C.F.R. 106.44, the Title IX formal complaint and grievance process does not prevent a principal from immediately removing a student respondent from the educational program or activity on an emergency basis, provided that the principal: (1) informs the Title IX Coordinator of the alleged act, and (2) conducts an individualized safety and risk analysis and determines that emergency removal is necessary in order to protect a complainant or other student or individual from an immediate threat to physical health or safety. In the event that an emergency removal of a student respondent is necessary, the principal should comply with the Student Code of Conduct provisions regarding suspension and expulsion of students in order to provide respondent with the appropriate notice and opportunity to challenge the decision.

Emergency removal does not modify any rights under the Individuals with Disabilities Education Act (IDEA), Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act.

K. False Statements and Allegations

The Board's sexual harassment policies and procedures prohibit anyone from knowingly making false statements or knowingly submitting false information during the sexual harassment complaint procedures. A student who deliberately, recklessly, and falsely accuses another student and/or employee of a violation of this policy will be subject to disciplinary sanctions as outlined in the Code of Student Conduct.

L. Record-keeping

All records shall be maintained in accordance with 34 C.F.R. § 106.45(b)(10). Specifically, the school system will keep records related to reports of alleged sexual harassment for a minimum of seven (7) years, including investigation records, disciplinary sanctions, remedies, appeals, and records of any action taken, including supportive measures. If supportive measures are not offered in response to a report, the records retained should document why supportive measures were not offered.

Student Sexual Harassment Complaint Form

This form may be used by a student, a student's parent or guardian, or an individual acting on a student's behalf who believes the student is a victim of sexual harassment to submit a complaint regarding sexual harassment (Board Policy 5.281 Student Sexual Harassment). This form should be submitted to the principal of the school. However, if the complaint concerns the principal, the complaint may be made directly to the Title IX Coordinator or the Superintendent.

Student's Name: _____ School: _____

Grade: _____

Name of Person Completing the Form (if not the student) _____

Your Home Phone: _____

Your Home Address: _____

Describe the sexual harassment, including all pertinent facts supporting the complaint.

_____

_____

_____

_____

(Attach additional paper, if needed.)

When did this happen (over what time period if continuing or more than once):

_____

_____

_____

_____

(Attach additional paper, if needed.)

Identify the person(s) whose actions led to the filing of the complaint, and all witnesses or other persons having information that is relevant to the complaint.

_____

_____

_____

_____

(Attach additional paper, if needed.)

Do you have suggestions for resolving this situation? If so, list them here:

_____

_____

_____

_____

(Attach additional paper, if needed.)

Attach copies of documents or other evidence that is relevant to the complaint.

I affirm that to the best of my knowledge, the foregoing information is true, accurate, and complete.

Signature: _____ Date: _____

WEBSITE ACCESSIBILITY

The Mobile County Public School System is committed to ensuring that the content on its website it accessible to everyone, including those with disabilities and users of assistive technology.

Grievances related to Section 504, Title II or other formal grievances can be filed with the System using the procedures outlined in the Section 504 Grievance Procedures located on the Board's website.

Reference: Web Content Procedures
(located on the Board's website)

Legal Reference: Section 504 (Rehabilitation Act) and Title II (American with Disabilities Act)
Date Adopted: January 24, 2018

SERVICE ANIMALS

The Mobile County Public School System permits individuals with disabilities to use their service animals as allowed by law and pursuant to the System's procedures relating thereto.

Legal Reference: Title II of the Americans with Disabilities Act: Alabama Code - §21-7-4
Date Adopted: February 26, 2018

PROCEDURES FOR USE OF SERVICE ANIMALS

The Mobile County Public School System permits individuals with disabilities to use their service animals. A "service animal" is a dog that has been individually trained to do work or perform tasks for an individual with a disability. The tasks performed by the dog must be directly related to the person's disability. Emotional support animals are not service animals.

If a particular service animal is out of control or if it poses a direct threat to the health and safety of others, or if it is not housebroken, it may be excluded.

The service animal must be harnessed, leashed or tethered unless these devices interfere with the service animal's work. In that case, the person must use voice, signal, or other effective means to maintain control of the animal.

Staff may not require documentation or proof that the service animal has been certified or trained, but service dogs are subject to the same licensing and vaccination rules that are applied to all dogs.

The Individuals with Disabilities Act (IDEA) and Section 504 of the Rehabilitation Act allow a student to use an animal that does not meet the above definition of "service animal" if that student's IEP or 504 team decides (on a case-by-case basis) the animal is necessary for the student to receive a free and appropriate education.

In the case of a disabled child (including a child diagnosed on the autism spectrum) any aide assigned to assist the child shall be trained with the service animal in basic commands in order to assist the child as a team.

All requests for an individual with a disability to be accompanied by a service animal shall be submitted in writing to the Superintendent's Office. Forms are available for this purpose.

MOBILE COUNTY PUBLIC SCHOOL SYSTEM

REQUEST TO BRING A SERVICE ANIMAL TO SCHOOL OR WORK

Date _____ (request made at least ten (10) days prior to animal's presence)

Name of Student/Employee/Individual Requesting to Bring Service Animal _____

Parent Name (if Student is making request) _____

School _____

Disability of Student/Employee/Individual _____

Describe the task that the service animal performs that is directly related to the individual's disability.

Documentation attached that the Service Animal is:

□ Properly and currently vaccinated and in good health.
□ Under the control of a properly trained handler. Name of handler: _____

Submit Request to Superintendent's Office. If the request is being made on behalf of a student with a disability, the student's 504/IEP Team will meet to address the request.

Note: ANNUAL APPLICATION AND REVIEW REQUIRED

MOBILE COUNTY PUBLIC SCHOOL SYSTEM

SERVICE ANIMAL REGISTRATION/AGREEMENT

_____ _____

Owner Student (if applicable)

□ Request Form is attached

Documentation attached that the Service Animal is:

□ Properly and currently vaccinated and in good health.
□ Under the control of a properly trained handler. Name of handler: _____

I have read and understand the Mobile County Public School System's Service Animal Policy 3.33 and I will abide by this Policy.

I understand that if my Service Animal is out of control or the animal's handler does not effectively control the animal's behavior or the animal is not housebroken or the animal's presence poses a direct threat to the health or safety of others, the School System has the discretion to exclude or remove the service animal from its property.

I agree to be responsible for any and all damage to school property, personal property, and any injuries to individuals caused by the service animal. Further, I agree to indemnify, defend and hold harmless the Mobile County Public School System and its Board Members and employees from and against any and all claims, actions, suits, judgements and demands brought by any party arising on account of, or in connection with, any activity or damage or injury caused by the service animal.

OWNER OF SERVICE ANIMAL

_____

Signature

Date: _____

Note: This Registration/Agreement is valid until the end of the current school year. It must be renewed prior to the start of each subsequent school year or when a different service animal will be used.

SAFETY

A comprehensive safety plan complying with State Department of Education guidelines will be developed, implemented and periodically reviewed.

School principals and employees with supervisory authority over specific departments and sites should keep safety a high priority and principals should work with the appropriate divisions to develop a property safety program for each school. The principal also will assume the responsibility for reporting to the appropriate divisions safety needs as they might arise.

The Facilities Division will work with the building administrators to assist in the implementation and observance of applicable fire codes. In addition, the Facilities Division will cooperate with other divisions in the development of fire prevention and safety procedures such as emergency drills and personnel training. A uniform emergency drill program is to be developed and maintained, addressing such emergencies as fire, storm, crisis, student disruption for all departments throughout the School System.

Safety inspections will be included in the regular maintenance program for the school system.

The superintendent is authorized to close a school if prevailing or potential hazards threaten the safety and well-being of students or employees.

Law enforcement agencies shall be authorized to make periodic visits to local schools to the extent authorized by law to detect the presence of illegal drugs, unannounced to anyone except the local superintendent and building principal.

Legal Reference: Alabama Administrative Code § 290-3-1-.02(1)(b)(1), as amended.

Date Adopted: December 11, 2007
Hearing Dates: March 19, 2013; March 25, 2013
Date Amended: March 25, 2013

TOBACCO USE

Smoking and the use of tobacco products including electronic type cigarettes (or "e-cigarettes) are prohibited on school grounds and at school activities.

Student and employee violations will be disciplined in accordance with the existing disciplinary procedures. Employees who violate this policy shall be subject to discipline including the possibility of suspension or termination. Visitors in violation of this policy will be asked to leave the premises.

The term "smoking" as used herein includes carrying or holding a lighted pipe, cigar or cigarette of any kind (including e-cigarettes), or any other smoking paraphernalia, as well as emitting or exhaling the smoke of a pipe, cigar or cigarette of any kind.

Electronic cigarettes (e-cigarettes or e-cigs) are battery-operated devices that deliver nicotine, flavor additives and other chemicals through a vapor that is inhaled by the user.

The term "tobacco product" as used herein includes the use of any type of tobacco product, such as chewing tobacco, snuff, or any other tobacco product that is ordinarily lit, inhaled, chewed or otherwise placed in one's mouth or nose.

Legal Reference:

Public Hearings: **February 11, 2015**
February 19, 2015

Date Amended: March 25, 2013

Firearm Possession

The possession of a firearm by an individual, employee, visitor, or student inside or on any property owned, leased, or operated by the Mobile County Public School System is strictly prohibited except for those individuals who lease undeveloped system property for hunting or sporting activities. Otherwise, possession of a firearm is strictly prohibited whether or not those individuals, employees, visitors or students possess a legal permit to carry said firearm or if the individual possessing the firearm is licensed to do so by the State of Alabama or any other state. Duly sworn and trained peace officers in the performance of their duties are exempted from this prohibition. Employees who violate this policy are subject to discipline up to and including the possibility of termination. Students shall be disciplined for the possession of firearms to the extent required by law, including, but not limited to Code of Alabama Section 16-1-24.3, as amended.

Legal Reference: Code of Alabama § 16-1-24.3, as amended; Alabama Administrative Code § 290-3-1-.02 (1)(b)(3), as amended.

Adopted: February 7, 2001
Public Hearings: March 19, 2013, March 25, 2013
Revised: May 25, 2010, March 25, 2013

COMPUTER, INTERNET AND ELECTRONIC COMMUNICATION ACCEPTABLE USE

MCPSS relies on its computer network to conduct its business. To ensure that MCPSS Computer Resources are used properly by its employees, students, independent contractors, agents, vendors and other computer Users (the "Users"), the Board of School Commissioners for MCPSS has created and passed has created this Computer Use Policy (the "Policy"). The rules and obligations described in this Policy apply to all Users (the "Users") of MCPSS' computer network or Computer Resources, wherever they may be located

MCPSS' policies against discrimination and harassment (sexual or otherwise) apply fully to MCPSS' Computer Resources and Resources, and any violation of those policies is grounds for discipline up to and including termination. Students who violate these policies are subject to disciplinary action consistent with Board policy and the Student Handbook. Vendors, consultants and other third parties must adhere to these policies and are subject to losing their right to access MCPSS Computer Resources for violations of these policies.

The term *Computer Resources* as used herein refers to MCPSS' entire computer, electronic and communications network. Specifically, the term *Computer Resources* includes, but is not limited to: computers, host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, tablets such as IPAD's, telephones, facsimile machines, scanners, software, data files, peripherals such as printers, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, e-mail systems) that may be accessed directly or indirectly (including access by Students, vendors, consultants and other third parties using personally owned computer hardware as authorized by MCPSS) from our computer network or that are owned or have been purchased by MCPSS.

The Computer Resources are the property of MCPSS and may be used for only legitimate business and educational purposes. Users are permitted access to the Computer Resources to assist them in performance of their jobs. Computer and internet access is provided for MCPSS business *use,* but *occasional* minimal personal use is allowed. Use of the Computer Resources is a privilege that may be revoked at any time. Users who violate this Policy may have their Computer/Internet use privileges revoked at any time and without prior notice AND are subject to discipline up to and including the possibility of termination.

In using or accessing the Computer Resources, Users must comply with and be aware of the following provisions:

No Expectation of Privacy. The computers and computer accounts given to Users are to assist them in the performance of their jobs or in the case of students, in their educational studies and activities. Users should not have an expectation of privacy in anything they create, store, send or receive on the Computer Resources. Computer Resources belong to MCPSS and may be used only for the purposes set forth herein. MCPSS has the right, but not the duty, for any reason and without the permission of any User, to monitor any and all of the aspects of its Computer Resources, including, without limitation, reviewing documents created and stored on its Computer Resources, deleting any matter stored in its system, monitoring sites visited by Users on the Internet, monitoring chat and news groups, reviewing material downloaded or uploaded by Users from the Internet, and reviewing E-Mail sent and received by Users. Employees and Users should not have an expectation of privacy in anything they create, store, send or receive using the Computer Resources.

Waiver of privacy rights. MCPSS reserves the right to inspect the contents of all electronic data stored on MCPSS computer equipment or Computer Resources. Users, in using MCPSS Computer Resources, expressly waive any right of privacy in anything they create, store, send or receive on MCPSS Computer Resources or through the Internet or any other computer network. Users consent to allowing personnel of MCPSS to access and review all materials Users create, store, send or receive on the computer or through the Internet or any other computer network. Users understand that MCPSS may use human or automated means to monitor use of its Computer Resources, including data stored on the local drive, data stored on any network drive, and electronic mail.

Passwords. Users are responsible for safeguarding their passwords for access to the Computer Resources or Computer Resources. Individual passwords should not be printed, stored online or given to others. Users are responsible for all transactions made and actions taken using their passwords. No User may access the Computer Resources with another User's password or account. Use of passwords to gain access to the Computer Resources or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the Computer Resources.

Viruses and Virus Protection. Users may not disable or remove virus protection software. Viruses can cause substantial damage to Computer Resourcess. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into MCPSS' Computer Resources or computer network. Virus software updates are automatically distributed regularly to Computer Resources. Users may not interrupt the update process and must report any errors in the update process immediately to MCPSS' support help desk. PCs not attached to the LAN must be updated by the User. The Information Technology Department will provide virus updates.

Compliance with applicable laws and licenses. **In their use of Computer Resources, Users must comply with all software licenses, copyrights and all other state, federal and international laws governing intellectual property and online activities.** It is **MCPSS'** policy to comply fully with all software copyright licenses. Employees who willfully circumvent this policy will be subject to disciplinary action up to and including termination of employment. In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

Prohibited Activities. The following activities, items or materials are prohibited:

Inappropriate or unlawful material. Material that is fraudulent**,** harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups), downloaded from the Internet or displayed on or stored in MCPSS computers. This includes e-mails known as "Spam" and e-mails containing non business related matter. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

Without prior written permission from the Executive Manager of Information Technology. Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material or any other unauthorized use, including material or significant personal uses.

Using or copying software in violation of a license agreement or copyright. Violating any state, federal or international law.

Waste of Computer Resources. Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet playing games, engaging in online chat groups, printing multiple copies of documents or otherwise creating unnecessary network traffic.

Accessing other User's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. The ability to read, alter or copy a file belonging to another User does not imply permission to read, alter or copy that file. Users may not use the Computer Resources to "snoop" or pry into the affairs of other Users by unnecessarily reviewing their files and e-mail. Excepted from this provision are those persons conducting investigations or administrative duties at the request and with the authorization of the Executive Manager of Information Technology or Executive Manager of Human Resources.

Misuse of software. Without prior written authorization from the Executive Manager of the Information Techonology Department, Users may not do any of the following:

(1) Copy software for use on their home computers;
(2) provide copies of software to any independent contractors or third party;
(3) install software on any MCPSS workstations or servers;
(4) download any software from the Internet or any other online service to any MCPSS workstations or servers;
(5) modify, revise, transform, recast or adapt any software or reverse-engineer, disassemble or decompile any software. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors; and
(6) Users who have currently copied software for home computers, distributed software or installed software on corporate computers are required to obtain approval according to the current guidelines or remove the software immediately.

If you become aware of someone using Computer Resources for any of these activities, you are obligated to report the incident immediately to your supervisor. Violations of any aspect of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

E-Mail Policy

To maximize the benefits of its Computer Resources and minimize potential liability, MCPSS has created this E-mail usage policy. All computer Users are obligated to use these resources responsibly, professionally, ethically and lawfully.

Employees and other Users are given access to our computer network to assist them in performing their duties. Employees and Users, including students, should not have an expectation of privacy in anything you create, store, send or receive on the Computer Resources. The Computer Resources belongs to MCPSS and may only be used for business purposes. Without prior notice, MCPSS may review any material created, stored, sent or received on its network or through the Internet or any other computer network**.**

Sending unsolicited e-mail (spamming). Without the express permission of their supervisors, employees may not send unsolicited e-mail to persons with whom they do not have a prior relationship.

Altering attribution information. Employees must not alter the "From:" line or other attribution-of-origin information in e-mail, messages or postings. Anonymous or pseudonymous electronic communications are forbidden. Employees must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, sending e-mail or otherwise communicating online.

Attorney-client communications. E-mail sent to in-house counsel, if any, or an attorney representing MCPSS should include this warning header on each page: "ATTORNEY-CLIENT PRIVILEGED; DO NOT FORWARD WITHOUT PERMISSION." Communications from attorneys may not be forwarded without the sender's express permission.

Confidential Transmissions. Any confidential e-mail, and/or files transmitted with it, is intended solely for the use of the individual or entity to whom it is addressed. The communication may contain material that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received an e-mail or communication in error, please notify the sender immediately.

Internet Use Policy

The Internet can be a valuable source of information and research. In addition, e-mail can provide excellent means of communicating with other employees, our customers and clients, outside vendors and other businesses. Use of the Internet, however, must be tempered with common sense and good judgment. Users who abuse their use of Computer Resources to access the Internet will may have access to the Internet restricted or removed. In addition, Users who violate this policy may be subject to disciplinary action, including the possibility of termination, student discipline (as applicable) and civil and criminal liability.

Your use of the Internet is governed by this policy:

Disclaimer of liability for use on Internet. MCPSS is not responsible for material viewed or downloaded by Users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

Employees' duty of care. Employees should endeavor to make each electronic communication truthful and accurate. You should use the same care in drafting e-mail / electronic documents as you would for any other written communication. Please keep in mind that anything created or stored on the Computer Resources may, and likely will, be reviewed by others.

Duty not to waste Computer Resources. Because audio, video and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related**.**

No privacy in communications. Users of MCPSS Computer Resources should never consider electronic communications to be either private or secure. E-mail may be stored indefinitely on any number of computers, including that of the recipient. Copies of your messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect usernames may be delivered to persons whom you never intended.

Monitoring of computer usage. MCPSS has the right, but not the duty, to monitor any and all aspects of its Computer Resources, including, but not limited to, monitoring sites visited by Users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by Users to the Internet and reviewing e-mail sent and received by Users.

Blocking of inappropriate content. MCPSS may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by MCPSS networks. In the event you, nonetheless, encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to MCPSS blocking software.

Games and entertainment software. Users may not use MCPSS' Internet connection to play games, download games or other entertainment software including screen savers. Educational games approved by the teacher and or administration of the MCPSS are excepted from this provision.

Illegal copying. Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages and other material you wish to download or copy.

Accessing the Internet. To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to MCPSS' network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited.

Prohibited Activities. The prohibited activities referenced above are also prohibited in connection with Users of MCPSS' Computer Resources use of the internet. Users must avoid internet websites and locations that are ***harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate while using MCPSS Computer Resources.***

Students

The board supports access by students to rich information resources and the development by staff of appropriate skills to analyze and evaluate such resources.

All such materials shall be consistent with board-system guidelines and staff will provide guidance and instruction to students in the appropriate use of such resources.

Annually, students and parents will be given MCPSS' guidelines and rules governing procedures for acceptable use of the Internet describing the information available and prohibited uses of system computers. Students and parents must sign a written statement acknowledging the guidelines in order for the student to access the Internet at school.

In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. In compliance with federal law, the online activities of minors **will** be monitored.

Employees

Employees will be provided a copy of the MCPSS acceptable use guidelines and sign a statement that they agree to the terms.

See also Board Policy 6.12

References – Procedures: *Computer,* Internet *and Electronic Communication* Acceptable Use
Date Adopted: December 11, 2007
Public Hearings: March 19, 2013, March 25, 2013
Amended: March 23, 2011, March 25, 2013

PROCEDURE:
INTERNET ACCEPTABLE USE

In order to match electronic resources as closely as possible to the approved district curriculum, district personnel must comply with Board Policy IFAC governing the selection of instructional materials. In this manner, school personnel will provide developmentally appropriate guidance to students as they make use of Internet resources to conduct research and other studies related to the district curriculum. All students will be informed by teachers of their rights and responsibilities as users of telecommunication networks prior to gaining access to any network service, either as an individual user or as a member of a class or group.

As much as possible, access to Internet information resources will be designed in ways which point students to those resources that have been reviewed and evaluated by the teacher prior to use. Since students may be able to move beyond those resources to others which have not been evaluated by teachers, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Students may pursue research on the Internet independent of teacher supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

With the complex networking and easy access to systems available worldwide through the Internet, users and the parents of users should understand that school district personnel cannot control the content of information residing on Internet. Users and parents of users should be advised that some locations on the Internet may contain materials considered to be defamatory, inaccurate, abusive, obscene, sexually oriented, or illegal. The Mobile County Public School System does not condone the use of such materials and does not permit usage of such material in the school environment. Parents should be aware of the existence of such materials and monitor home usage of the Internet (if available). Students bringing such materials into the school environment will be dealt with according to the Code of Conduct along with the termination of access privileges.

Core Rules for Use of Internet

The use of Internet resources is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges as well as punishment for such violations as prescribed in the Code of Conduct. Unacceptable uses of Internet include the following:

- Using profanity or obscenity.

- Copying and/or distributing commercial software in violation of copyright law.

- Ordering services or merchandise from other agencies that have Internet access. All matters concerning the merchandise and services ordered from a seller, including but not limited to purchase terms, payment terms, warranties, guarantees, maintenance and delivery, are solely between the seller and the user. The Mobile County Public School System makes no warranties or representations whatsoever with regard to any goods or services provided by the seller and expressly forbids these transactions originating from the school system Internet access. The Mobile County Public School System and school system personnel shall not be a party to these transactions or be liable for any costs or damages arising out of the actions of sellers.

- Using the network for financial gain, for commercial activity, or for any illegal activity.

- Altering and forwarding personal communication without the author's prior consent.

- Spoofing or otherwise attempting to send anonymous messages of any kind.

- Lending your password to other students and\or adults.

- Using the network to access a file that contains pornography, inflammatory material, inappropriate material, or any material not specifically related to the instructional lesson, objective, or assignment.

- Using copyrighted materials in reports without permission.

- Publicizing your home address or phone number.

- Creating a computer virus and placing it on the network.

- Using the network for sending and receiving a large number of personal messages.

- Using the network to send/receive inflammatory messages.

All users should be aware that the inappropriate use of Internet information resources can be a violation of local, state, and federal laws.

STUDENT CONTRACT REGARDING THE USE OF INTERNET

I, _____, accept and agree to abide by the following legal rules.

I agree to abide by all rules which are listed in the Mobile County Public School System Procedures for Internet Use.

I realize that the primary purpose of the Mobile County Public School System's Internet connection is educational, and that as such, educational purposes shall take precedence over all others.

I realize that the use of Internet is a privilege, not a right. I accept that inappropriate behavior may lead to penalties, including revoking of Internet access, disciplinary action, and/or legal action.

I agree not to participate in the transfer of inappropriate or illegal materials through the Mobile County Public School System's Internet connection. I realize that in some cases the transfer of such material may result in legal action against me.

I agree not to allow other individuals to use my account for Internet activities nor will I give anyone my password.

I agree not to download any shareware or freeware programs from the Internet.

I agree not to bring software from home into the computer lab or library media center.

Signed_____

Date_____

Please complete and return this form if you agree to allow your child access to the Mobile County Public School System's Internet connection.

PARENTAL CONTRACT REGARDING THE USE OF INTERNET

As the parent or guardian of this student, I have read the terms and conditions for system Internet access privileges. I understand this access is for educational purposes and that the Mobile County Public School System has taken available precautions in forewarning and educating all interested parties of the controversial material that is accessible on the Internet. I also recognize that it is impossible for the Mobile County Public School System to restrict access to all controversial materials. I will not hold the Mobile County Public School System nor its employees responsible for materials acquired by my son/daughter on the network in violation of the Internet Acceptable Use Policy and Procedures for Internet Acceptable Use. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting.

I hereby give my permission to the Mobile County Public School System to issue Internet access privileges to my son/daughter.

Signed _____

Date _____

COPYRIGHT

The board encourages its staff to enrich the learning program by making proper use of supplementary materials. The staff is responsible for abiding by MCPSS copying procedures and obeying the requirements of the law. In no circumstances shall it be necessary for MCPSS staff to violate copyright requirements in order to perform their duties properly.

Any staff member who is uncertain as to whether reproducing or using copyrighted material complies with the MCPSS's procedures or is permissible under the law should contact the MSPSS library media services. The library media services department will also assist staff in obtaining proper authorization to copy or use protected material when such authorization is required.

Date Adopted: December 11, 2007

PROFESSIONAL PUBLISHING

Employees publishing written materials concerning the school system shall have the superintendent's approval. Written materials developed by board employees in their official capacity as a board employee for the school system other than for personal use shall be the property of the school system and not that of the individual writers.

Date Adopted: December 11, 2007

DATA USE AND GOVERNANCE POLICY

The Mobile County Public School System Data Use and Governance Policy is based upon, but not limited to, maintaining compliance with the Family Educational Rights and Privacy Act (FERPA) as well as the Alabama Data Breach Notification Act of 2018. The Superintendent is authorized to establish, implement, and maintain data use and governance measures. These measures shall include establishing data security classifications; implementing procedural, physical, and electronic security controls; managing external data requests; maintaining records regarding security access and establishing a Data Governance Committee. The data governance measures will apply to Board employees and all Board operations. In addition, this policy will apply to all individuals who are granted access to data in conjunction with any services that they provide at the request of the Board. Any unauthorized access, use, transfer, or distribution of Board data by an employee, student, or other individual, may result in disciplinary action that may include a recommendation for termination and other legal action.

Legal References:

Alabama Data Breach Notification Act of 2018

Family Educational Rights and Privacy Act (FERPA)

Policy Adopted: February 22, 2017

Policy Revised: May 23, 2024

Reference Procedures: Data Governance Internal Procedures

Mobile County Public School System

Data Governance
Internal Procedures

The following documents are affiliated with Mobile County Public School System Data Governance procedures, training, and guidance.

Contents

STATE MONITORING CHECKLIST CROSS-REFERENCE 3

APPLICABLE LAWS AND STANDARDS 4

DATA USE AND GOVERNANCE POLICY AND PROCEDURES 6

DATA GOVERNANCE COMMITTEE 7

DATA SECURITY MEASURES 8

I. PURPOSE 8
II. SCOPE 8
III. GUIDING PRINCIPLES 9
IV. ACCESS COORDINATION 9
V. DATA CLASSIFICATION 10
VI. COMPLIANCE 17
VII. IMPLEMENTATION OF NETWORK/WORKSTATION CONTROLS AND PROTECTIONS AND PHYSICAL SECURITY 17
VIII. TRANSFER OF DATA TO EXTERNAL SERVICE PROVIDER 20

DATA GOVERNANCE TRAINING 21

I. SCHOOL AND CENTRAL OFFICE ADMINISTRATORS 21
II. SCHOOL REGISTRAR DATA SECURITY TRAINING 21
III. TEACHER AND STAFF TRAINING 21
IV. PARENT AND BOOSTER TRAINING 21

DATA QUALITY CONTROLS 22

I. JOB DESCRIPTIONS 22
II. SUPERVISORY RESPONSIBILITIES 22

STUDENT INFORMATION SYSTEMS 22

I. STUDENT INFORMATION APPLICATIONS 22
II. POWERSCHOOL ACCESS 23

POWERSCHOOL PERMISSION STANDARDS FOR MOBILE COUNTY PUBLIC SCHOOL SYSTEM 27

I. PERMISSION COMMITTEE 27
II. ALLOWABLE POWERSCHOOL PERMISSION SETTINGS 28
I. POWERSCHOOL SUBSTITUTE TEACHER SET UP & ROLES 31

EMAIL USE AND SECURITY AGREEMENT 33

I. USER AGREEMENT 33
II. MOBILE COUNTY PUBLIC SCHOOL SYSTEM EMAIL DISCLAIMER 33

BANKING SECURITY **33**

I. ACH TRANSFERS 33
II. BANK BALANCE AUDITING RECOMMENDATIONS FOR PREVENTING ELECTRONIC THEFT 33

DATA BACKUP AND RETENTION PROCEDURES **34**

I. PURPOSE OF DATA BACKUP AND RETENTION PROCEDURES 34
II. SCOPE 34
III. GENERAL SYSTEM DATA BACKUP PROCEDURES 35
IV. E-MAIL DATA BACKUP PROCEDURES 35
V. TIME FRAMES FOR DATA RETENTION 36
VI. EMAIL ARCHIVING 37
VII. DATA INCLUDED / EXCLUDED 37
VIII. RESPONSIBILITY OF DATA BACKUP AND DATA RETENTION 37
IX. DATA RESTORE PROCEDURES 38
X. SYSTEMS TABLE I 38
XI. SYSTEMS TABLE II 39

ALABAMA DATA BREACH NOTIFICATION ACT OF 2018 **39**

DATA PROTECTION **39**

I. Data Protected for Employees 39

II. Before a Breach Occurs 40

III. After a Breach Occurs 40

EXHIBIT A: - IDENTITY THEFT TRAINING **42**

EXHIBIT B: COMPUTER, INTERNET, AND ELECTRONIC COMMUNICATION ACCEPTABLE USE **45**

IN USING OR ACCESSING THE COMPUTER RESOURCES, USERS MUST COMPLY WITH AND BE AWARE OF THE FOLLOWING PROVISIONS: **46**

EXHIBIT C: COPIER MACHINE SECURITY RECOMMENDATIONS **51**

PROVISIONS FOR CONSIDERATION – NOT YET IMPLEMENTED **53**

ELECTRONIC SIGNATURE AGREEMENT (NOT IMPLEMENTED) 53
RESTRICTIONS ON PARENTS POSTING IMAGES OF STUDENTS (WHO ARE NOT THEIR OWN CHILDREN) TO SOCIAL MEDIA (NOT IMPLEMENTED) 54

State Monitoring Checklist Cross-Reference

	ON-SITE	INDICATORS	MCPSS Data Governance Plan
1.	Has the data governance committee been established and roles and responsibilities at various levels specified?	Dated minutes of meetings and agendas Current list of roles and responsibilities	See committee files Committee
2.	Have the local school board adopted a data governance and use procedures?	Copy of the adopted data governance and use policy Dated minutes of meetings and agenda	Internal Procedures
3.	Do the data governance procedures address physical security?	Documented physical security measures	Controls and Protections
4.	Do the data governance procedures address access controls and possible sanctions?	Current list of controls Employee policy with possible sanctions	General provisions Data transfers POWERSCHOOL Permissions Reporting breaches Data Security Agreements Email –Violations and Enforcement
5.	Do the data governance procedures address data quality?	Procedures to ensure that data are accurate, complete, timely, and relevant	Quality Controls
6.	Do the data governance procedures address data exchange and reporting?	Policies and procedures to guide decisions about data exchange and reporting Contracts or MOAs involving data exchange	Data transfers and Non-Disclosure Agreements Disclosure of data via email
7.	Have the data governance procedures been documented and communicated in an open an accessible way to all stakeholders?	Documented methods of distribution to include who was contacted and how Professional development for all who have access to PII	Dissemination of policy Data Security Training

Applicable Laws and Standards

MCPSS will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. MCPSS data governance procedures are informed by the following laws, rules, and standards, among others:

ALABAMA DATA BREACH NOTIFICATION ACT OF 2018

This Act is codified in the Commercial Law and Consumer Protection Title in Alabama Code § 8-38-1 and addresses any entity that maintains sensitive personally identifying information (SPII).

FERPA

The Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

ALABAMA RECORDS DISPOSITION AUTHORITY

Alabama Code Section 41-13-23 authorized the Alabama Department of Archives and History to publish rules for Local Government Records Destruction.

ALABAMA OPEN RECORDS LAW

COPPA

The Children's Online Privacy Protection Act, regulates organizations that collect or store information about children under age 13. Parental permission is required to gather certain information.

HIPAA

The Health Insurance Portability and Accountability Act, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

Payment Card Industry Data Security Standard (PCI DSS)

This standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. See www.PCI security standards.org for more information.

ISO Standards (http://www.iso.org/iso/home/standards.htm)

ISO 17799:2000 – Information technology – Code of practice for information security management

ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

Data Use and Governance Policy and Procedures

Policy History:

Current Policy: 3.53	Adopted: Pending Board Approval on May 30, 2024

The Mobile County Public School System Data Use and Governance Policy is based upon, but not limited to, maintaining compliance with the Family Educational Rights and Privacy Act (FERPA) as well as the Alabama Data Breach Notification Act of 2018. The Superintendent is authorized to establish, implement, and maintain data use and governance measures. These measures shall include establishing data security classifications; implementing procedural, physical, and electronic security controls; managing external data requests; maintaining records regarding security access and establishing a Data Governance Committee. The data governance measures will apply to Board employees and all Board operations. In addition, this policy will apply to all individuals who are granted access to data in conjunction with any services that they provide at the request of the Board. Any unauthorized access, use, transfer, or distribution of Board data by an employee, student, or other individual, may result in disciplinary action that may include a recommendation for termination and other legal action.

Reference: Data Governance Internal Procedure

Legal Reference: Alabama Data Breach Notification Act of 2018

Legal Reference: FERPA Law

Date of Adoption: May 30, 2024

Data Governance Committee

Name	Department
David K. Akridge, Executive Director of Technology	Technology
Dr. Ursula D. Martin, Technology Coordinator *designated as coordinator of security under the Alabama Data Breach Notification Act 2018	Technology
Charles B. Martin, Student Data Manager (Data Governance Manager)	Technology
Andy Berry, Network Manager	Technology
Neal Sizemore, Network Exchange Specialist	Technology
Terrence Mixon, Executive Director, Student Services	Student Services
Curtess Belson, Student Services Supervisor	Student Services
Dr. Susan Hinton, Research, Accountability, Assessment, and Grants	Academic Affairs
Bryan Hack, Executive Director for Human Resources	Human Resources
POWERSCHOOL Permission Committee	
Charles B. Martin, Student Data Manager (Data Governance Manager)	Technology
Andy Berry, Network Manager	Technology
Curtess Belson, Student Services Supervisor	Student Services
Karen Baars, PowerSchool Support Specialist	Technology
Darla Langham, Information Support Specialist	Student Services
Angela V. Lincecum, Principal	Shepard Elem School
Rashad Stallworth, Principal	Scarborough Model Middle School
Timothy L. Hardegree, Principal	Theodore High School

Data Security Measures

I. Purpose

(A) Implement standards and procedures to effectively manage and provide necessary access to System Data, while at the same time ensuring the confidentiality, integrity and availability of the information. Insofar as these procedures deal with access to Mobile County Public School System computing and network resources, all relevant provisions in the Acceptable Use Policies are applicable.

(B) Provide a structured and consistent process for employees to obtain necessary data access for conducting Mobile County Public School System operations.

(C) Define data classification and related safeguards. Applicable federal and state statutes and regulations that guarantee either protection or accessibility of System records will be used in the classification process.

(D) Provide a list of relevant considerations for System personnel responsible for purchasing or subscribing to software that will utilize and/or expose System Data.

(E) Establish the relevant mechanisms for delegating authority to accommodate this process at the school level while adhering to separation of duties and other best practices.

II. Scope

(A) These Security Measures apply to information found in or converted to a digital format. (The same information may exist in paper format for which the same local policies, state laws, statutes, and federal laws would apply, but no electronic control measures are needed.)

(B) Security Measures apply to all employees, contract workers, volunteers, and visitors of the Mobile County Public School System and all data used to conduct operations of the System.

(C) Security Measures do not address public access to data as specified in the Alabama Open Records Act.

(D) Security Measures apply to System Data accessed from any location; internal, external, or remote.

(E) Security Measures apply to the transfer of any System Data outside the System for any purpose.

III. Guiding Principles

(A) Inquiry-type access to official System Data will be as open as possible to individuals who require access in the performance of System operations without violating local Board, legal, Federal, or State restrictions.

(B) The Superintendent and/or his/her designees shall determine appropriate access permissions based on local policies, applicable laws, best practices, and the Alabama Open Records Act.

(C) Data Users granted "create" and/or "update" privileges are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the System Data they create, update, and/or delete.

(D) Any individual granted access to System Data is responsible for the ethical usage of that data. Access will be used only in accordance with the authority delegated to the individual to conduct Mobile County Public School System operations.

(E) It is the express responsibility of authorized users to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(F) These Security Measures apply to System data regardless of location. Users who transfer or transport System data "off-campus" for any reason must ensure that they are able to comply with all data security measures prior to transporting or transferring the data.

IV. Access Coordination

(A) Central Office Department heads, supervisors, area specialists, and principals (Authorized Requestors) will assist in classifying data sensitivity levels for their areas of expertise and in identifying which employees require access to which information in order to complete their duties.

(B) The System Technology Coordinator and Student Data Manager will designate individuals within the technology department to implement, monitor, and safeguard access to System Data based on the restrictions and permissions determined by the Authorized Requestors using the technical tools available.

(C) Central Office Department heads, supervisors, area specialists, and principals will be responsible for educating all employees under their supervision of their responsibilities associated with System Data security.

V. Data Classification

(A) Mobile County Public School System's Data shall be classified into three major classifications as defined in this section. Requests for changes to the established data sensitivity classification or individual permissions shall come from the above identified Authorized Requestors to the Technology Department.

1) Class I – Public Use
This information is targeted for general public use. Examples include Internet website content for general viewing and press releases.

2) Class II – Internal Use
Non-Sensitive (See Class III) information not targeted for general public use.

3) Class III – Sensitive
This information is considered private and must be guarded from unauthorized disclosure; unauthorized exposure of this information could contribute to identity theft, financial fraud, breach of contract and/or legal specification, and/or violate State and/or Federal laws.

(B) FERPA Directory Information
Information disclosed as 'directory information' may fall into either Class I or Class II, depending
on the purpose of the disclosure. The following is MCPSS's list of which student information
is to be considered 'directory information'.

Mobile County Public School System FERPA Directory Information Disclosure
Updated to include MCPSS student number on May 6, 2014

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Mobile County Public School System, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, Mobile County Public School System may disclose appropriately designated 'directory information' without written consent, unless you have advised MCPSS to the contrary in accordance with MCPSS procedures. The primary purpose of directory information is to allow the Mobile County Public School System to include this type of information from your child's education records in certain school publications. Publications may be in print or digital format.
Examples include, but are not limited to, the following:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and

- Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks, take school pictures, or process data.

In addition, two federal laws require local educational agencies (LEAS) receiving assistance under the *Elementary and Secondary Education Act of 1965* (ESEA) to provide military recruiters, and institutions of higher learning, upon request, with three directory information categories – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.

MCPSS may disclose the following information as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended
- A student number assigned by MCPSS (in some cases*)

* In order to make certain software applications available to students and parents, MCPSS may need to upload specific 'directory information' to the software provider in order to create distinct accounts for students and/or parents. Examples of these include, but are not limited to PayPams.com, Moodle.com, and various education software applications. In these cases, MCPSS will provide only the minimum amount of 'directory information' necessary for the student or parent to successfully use the software service.

Data Classifications for Students

Student Data	Classification	Authorized Users	Web Access
Student Name*	Class I or II, depending on use	All, as needed	First Name, Last Initial only, except in press release, school newspaper, or C2C
MCPSS Student Number	Class II	Principal, Asst. Principal, Counselor, Registrar, Teachers, Student, Parent, CNP, Media Specialist. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
State Student Number*	Class II	Principal, Asst. Principal, Counselor, Registrar Student, Parent. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
Social Security Number*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker	No
Home Phone Number	Class I or II, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers. School directories with parental permission being first obtained. Rapid notification system directory.	No

Home Address	Class I, II, III, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers	No
Ethnicity*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers and After School Care workers. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
National School Lunch Program Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, CNP Coordinator and staff, Immediate teacher, (Point of Sale transactions will be done in such a way as to not identify students who receive free or reduced lunches. Cafeteria managers and CNP employees who process F/R applications or lists of benefit recipients will ensure the information is secure and made available only those persons who require it.)	No
ESL Status*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, ESL Supervisor, ESL Dept. employees, Assigned Teachers and After School Care workers. Also export to approved service providers in order to establish unique identities or	No

		accounts – requires Data Governance Committee approval.	
Special Ed Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
Medical Conditions	Class III, except in emergencies	Principal, Asst. Principal, Registrar, Nurse, Immediate Teacher, Lunch Room personnel (if food allergy), and After School Care workers, if applicable	No
Grades	Class III, except when used in conjunction with honor rolls/awards	Principal, Asst. Principal, Registrar Immediate Teachers, Student, Parents or legal guardian, School Counselor, Gifted Teacher (only for students assigned), PST Committees, Appropriate Central Office Administrators, Testing Coordinator, Transfer to schools and Scholarship applications, C2C	POWERSCHOOL Parent Portal - Access is to be given to parents or legal guardians only. POWERSCHOOL Teacher web access
Attendance*	Class III	Principal, Asst. Principal, Attendance Clerk, Registrar, Student Services Coordinator and staff, Truancy Officers, School Resource Officers, Immediate Teachers, PST Committee	POWERSCHOOL Parent Portal only
Discipline*	Class III	Principal, Asst. Principal, Counselor, SRO, Registrar, Student Services, PST Committee, School Resource Officers	No
Standardized Test Scores*	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing	No

		Coordinator, Appropriate Central Office Administrators, PST Committee, Student, Parent	
System Benchmark Test Scores	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Administrators, PST Committee, Student, Parent	No
*ALSDE may access all such information for State Reporting Collection purposes			

Data Classifications for Employees

Student Data	Classification	Authorized Users	Web Exposure
Employee Name*	Class I or II, depending on use	Human Resources, Principal, POWERSCHOOL data manager	Yes
MCPSS Employee Number	Class II	Principal, Payroll, Human Resources, and Maintenance staff, as needed	No
Social Security Number*	Class III	Human Resources, Payroll, Principal, POWERSCHOOL data manager	No
Home Phone Number	Class II	Human Resources, Principal, POWERSCHOOL data manager, school directories with employee permission, Rapid notification system directory	No
Home Address	Class III	Human Resources, Principal, POWERSCHOOL data manager	No
Ethnicity*	Class II	Human Resources, Principal	No
Medical Conditions	Class III	Human Resources, Principal	No
Certifications*	Class II	Human Resources, Principal, Payroll	No

Attendance	Class III	Human Resources, Payroll, Principal	No
Evaluations*	Class III	Human Resources, Principal	No
College or school transcripts or grades	Class III	Human Resources, Principal	No
HQT Status*	Class II	Human Resources, Principal, Asst. Principal, Registrar, Appropriate Central Office Administrators	Only as needed to comply with any Federal Programs reporting requirements
Prof. Dev. Records*	Class II	Human Resources, Principal, Asst. Principal, Registrar, PD Supervisor, Appropriate Central Office Administrators	No
Benefits	Class III	Human Resources and Payroll Staff	No
Salaries*	Class II	Human Resources, Principal, Asst. Principal, Registrar, Appropriate Central Office Administrators	Schedules, but not individual salaries
*ALSDE may access all such information for State Reporting Collection purposes			

VI. Compliance

(A) Data Users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to Class III (Sensitive) data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure, or distribution of System Data in any medium is expressly forbidden; as is the access or use of any System Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

(B) Each employee at the System will be responsible for being familiar with the System's Data Security Policy and these Security Measures as they relate to his or her position and job duties. It is the express responsibility of Authorized Users and their respective supervisors to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(C) Employees, whether or not they are Authorized Users, are expressly prohibited from installing any program or granting any access within any program to Class III without notifying the Technology Department.

(D) Violations of these Data Security Measures may result in loss of data access privileges, administrative actions, and/or personal civil and/or criminal liability.

VII. Implementation of Network/Workstation Controls and Protections and Physical Security

(A) **Shared Responsibilities**

1) The Technology Department shall implement, maintain, and monitor technical access controls and protections for the data stored on the System's network.

2) System employees, including Authorized Requestors, shall not select or purchase software programs that will utilize or expose Class III data without first consulting the Technology Department to determine whether or not adequate controls are available within the application to protect that data. *(The exception to this would be any software program purchased or utilized by the Alabama State Department of Education. In this case, the Alabama State Department of Education shall take all security responsibility for data it accesses or receives from Mobile County Public School System.)*

3) The Technology Department staff and/or the Authorized Requestor will provide professional development and instructions for Authorized Users on how to properly access data to which they have rights, when necessary. However, ensuring that all employees have these instructions will be the shared responsibility of the supervisor(s) of the Authorized User(s) and the Technology Department.

4) Technical controls and monitoring cannot ensure with 100% certainty that no unauthorized access occurs. For instance, a properly Authorized User leaves their workstation while logged in, and an unauthorized person views the data in their absence. Therefore, it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.

(B) **Authorized Requestors**

1) Authorized Requestors (Section IV. A) are responsible for being knowledgeable in all policies, laws, rules, and best practices relative to the data for which they are granting access; including, but not limited to FERPA, HIPAA, etc.

2) Authorized Requestors shall be responsible for informing appropriate Technology Department personnel about data classifications in order that the Technology Department can determine the best physical and/or logical controls available to protect the data. This shall include:

    a. Which data should be classified as Class III
    b. Where that data resides (which software program(s) and servers)
    c. Who should have access to that data (Authorized Users)
    d. What level of control the Authorized User should have to that data (i.e. read only, read/write, print, etc.)

(C) **Location of Data and Physical Security**

1) Class III data shall be stored on servers/computers which are subject to network/workstation controls and permissions. It shall not be stored on portable media that cannot be subjected to password, encryption, or other protections.

2) Serving devices (servers) storing sensitive information shall be operated by professional network system administrators, in compliance with all Technology Department security and administration standards and policies, and shall remain under the oversight of Technology Department supervisors.

3) Persons who must take data out of the protected network environment (transport data on a laptop, etc.) must have the permission of their supervisor prior to doing so. Permission to do so will be granted only when absolutely necessary, and the person transporting the data will be responsible for the security of that data, including theft or accidental loss.

4) All servers containing system data will be located in secured areas with limited access.

5) MCPSS staff who must print reports that contain Class II or III data shall take responsibility for keeping this material in a secure location – vault, locked file

cabinet, etc. In addition, all printed material containing Class III documentation shall be shredded when no longer in use.

(D) **Disposal of Hardware containing System Data**

1) Prior to disposal of any computer, the user will notify the Technology Department. A technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.

2) All schools and departments which purchase or lease copy machines or multifunction printers will be expected to include provisions for the destruction of data on the device's hard drive or the destruction of the hard drive itself prior to disposing of the copier or MFP or its return the leasing agency.

(E) **Application of Network and Computer Access Permissions**

1) The Technology Department staff shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage, and access to all storage and transport mediums; including, but not limited to:

    a. Maintaining firewall protection access to the network and/or workstations.

    b. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing 'guest' wireless networks with limited network permissions.

    c. Implementing virus and malware security measures throughout the network and on all portable computers.

    d. Applying all appropriate security patches.

    e. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

2) Technology Department staff will apply protection measures based on the Data Classifications (see sections IV and V), including:

    a. Categorizing and/or re-classifying data elements and views.

    b. Granting selective access to System Data.

    c. Documenting any deviation from mandatory requirements and implementing adequate compensating control(s).

    d. Conducting periodic access control assessments of any sensitive information devices or services.

(F) **Sensitive Data as it pertains to Desktops/Laptops/Workstations/Mobile Devices**

1) Firewalls and anti-virus software must be installed on all desktops, laptops and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner.

2) Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers is prohibited, unless such information is encrypted in a Technology Department-approved encryption format.

3) The user responsible for the device shall take proper care to isolate and protect files containing sensitive information from inadvertent or unauthorized access.

4) Assistance with securing sensitive information may be obtained from school-level Technology Support Teachers with input from the Technology Department, as necessary.

VIII. Transfer of Data to External Service Provider

(A) Student Class I data, directory information, and, in some cases Class II data, may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes. Provide that:

1) The teacher follows the protocols for getting approval for the site to be used.

2) MCPSS notifies parents about their right to restrict their child's data from being shared with such sites annually via Code of Conduct/AUP.

3) The transfer of data is handled in a manner approved by the Technology Department, or is performed by the Technology Department.

(B) No Class III data, or FERPA protected educational records, will be transferred to an external service provider without prior approval of the Data Governance committee. Exception: Alabama State Department of Education.

(C) No school or department should enter into a contract for the use of any program that requires the import of MCPSS data without first consulting and receiving approval from the Data Governance committee.

(D) The Data Governance committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:

1) Contract
2) Designating the service provider as an "Official" as defined in FERPA
3) Memorandum of Understanding
4) Memorandum of Agreement
5) Non-Disclosure Agreement

Data Governance Training

I. School and Central Office Administrators

(A) School and Central Office Administrators will receive refresher training on FERPA and other data security procedures annually at principals´ meetings

(B) Principals and Central Office Administrators shall contact the Technology Coordinator, Student Data Manager or the Students Services Department when in doubt about how to handle Class II and III information

(C) Principals and Central Office Administrators will be kept aware of emerging issues pertaining
to data security.

II. School Registrar Data Security Training

(A) School registrars will be trained and refreshed on FERPA and other data security procedures annually.

(B) School registrars' adherence to the data security procedures will be monitored by the Technology Department through random audits.

III. Teacher and Staff Training

(A) All new teachers will complete training on all MCPSS technology policies, including how their use of technology is governed by FERPA and other data security procedures established by MCPSS.

(B) All department heads will be expected to educate their support staff on data governance as it applies to their department's work. This guidance will be communicated from the Data governance committee.

(C) All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.

IV. Parent and Booster Training

(A) School administrators shall educate PTOs, boosters, and other parent groups about FERPA and student confidentiality. For instance, organizations who intend to post information about the school's students or activities should not compromise the privacy of students in protective custody. Because the school cannot tell these groups which students may be in such situations, the organization should be cautioned about exposing any information or photos that could cause harm to students or their families.

(B) The Technology Department shall have procedures that include educational materials for booster organizations who wish to post their own websites. This shall include both FERPA and COPPA information.

Data Quality Controls

I. Job Descriptions

(A) Job descriptions for employees whose responsibilities include entering, maintaining, or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality, and completeness. This includes, but is not limited to: school registrars, counselors, special education staff, and CNP staff handling free and reduced lunch data.

(B) Teachers shall have the responsibility to enter grades accurately and in a timely manner.

(C) School administrators shall have the responsibility to enter discipline information accurately and in a timely manner.

II. Supervisory Responsibilities

(A) It is the responsibility of all Supervisors to set expectations for data quality and to evaluate their staff's performance relative to these expectations annually.

(B) Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department, including the State Department of Education, if applicable.

Student Information Systems

I. Student Information Applications

(A) Any software system owned or managed by MCPSS which is used to store, process, or analyze student 'educational records' as defined by FERPA shall be subject to strict security measures. These systems are:

1) PowerSchool SiS (POWERSCHOOL) – General student information system
2) PowerSchool Special Programs – Special Education information system
3) Heartland – Child nutrition information system

(B) Administrators with supervisory responsibilities over MCPSS's Student Information Systems shall determine the appropriate access rights to the data and enforce compliance with these roles and permissions.

II. POWERSCHOOL Access

POWERSCHOOL enables authorized users to access the application from anywhere they may have Internet access. In response to this anywhere/anytime access, the Data Governance Committee and its POWERSCHOOL permissions sub-committee have implemented the following:

(A) Strong password requirement for Network/POWERSCHOOL logins

(B) Data Security Agreements for those with POWERSCHOOL permissions who are not MCPSS Employees

PowerSchool SiS Data Security Agreement Memo

Date: (Date to be established)

To: Principals

From: Charles Martin

RE: Data Security and Data Security Agreement

As you know, our student employee data should be carefully protected. Not only is much of this information subject to FERPA and HIPAA, but it is also data which could be used for identity theft. In order to ensure that all staff members who have access to PowerSchool SiS (POWERSCHOOL) understand the important responsibilities that come with such access, we have prepared the attached PowerSchool SiS Data Security Agreement form.

Please read the document carefully and notice that it warns against removing personal data on students and employees from the workplace. This type of information should not be carried outside of your school on USB drives, disks, or on laptops. If any of these portable devices were to be lost or stolen, it could put the system at great risk.

Please make enough copies of this document for each of your staff who have POWERSCHOOL permissions to sign. Have them sign the form. Make them a copy of the signed form, and then forward the original to the Technology Department. This will include you, your assistant principals, your counselors, the school nurse, and a few others in your school. The registrars have already received and signed a copy at the recent Registrar's meeting.

If you have questions, please feel free to contact me.

Mobile County Public School System Data Security Agreement

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Mobile County Public School System' student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to, the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of MCPSS in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or MCPSS administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.

I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled. Please sign below to indicate you understand and agree to the above statements.

Printed Name	Signature
Date	Location

Data Security Agreement: Athletic – Quick Entry Edit Provision

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Mobile County Public School System' student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of MCPSS in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or MCPSS administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.

I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.

Athletic – Quick Entry Edit Provision

I understand that access to the Quick Entry Edit utility is being added to my permission so that I may rapidly identify student athletes per the directions provided by the AHSAA. I agree not to delegate this responsibility to others. I will be careful in selecting the Athletic field and the correct students so that school does not incur unintended insurance costs.

Please sign below to indicate you understand and agree to the above statements.

Printed Name/Title	Signature
Date	Location

(C) 'Notification of Risks' to school administrators and registrars

Notice of Risks Related to POWERSCHOOL Usage

POWERSCHOOL Access for Parent Volunteers

Some schools rely on parent volunteers to help greet visitors and locate students. Due to FERPA and other confidentiality expectations, volunteers cannot be granted POWERSCHOOL rights.

Concerns about Parent Volunteers Checking Students Out of School

Releasing a child from school into the care of someone else is a serious responsibility. Schools should carefully assess whether the information in POWERSCHOOL for this purpose is always up to date. In the past registrars have raised concerns that parents often change their minds about who can and cannot check out their children, but they don't necessarily notify the school in a timely manner. This makes the prospect of allowing parent volunteers who are unfamiliar with the current circumstances of various family situations to check out students an area of concern. Student Services will be providing recommendations regarding this important function.

Allowing Others to Use Another User's POWERSCHOOL Account to 'Give' them Greater Access is Prohibited

A user's POWERSCHOOL permission level is based on their job responsibilities. Violating FERPA can have serious consequences, including the loss of Federal Funding and other legal liabilities. Since we have a responsibility to protect our student and employee data from identity theft or other misuse, no one may log into POWERSCHOOL and allow others to use their access. Participating in this practice violates our Acceptable Use policies and Data Security Procedures.

The Technology Department will perform random scans to determine if the same POWERSCHOOL user id is in use concurrently on two separate computers and investigate these occurrences as warranted. Registrars who are using multiple machines have been instructed to notify Technology of this so that dual logins on specific IP addresses will not be viewed as a potential violation of this rule.

Plan for when your Registrar is Out for an Extended Period

You should have a plan for occasions when your registrar is out sick or on vacation. Anyone filling in for the registrar must be a MCPSS approved employee. Technology and/or Stu will attempt to help in extreme situations, but our ability to do so is limited.

Providing Information to Others on Students NOT Enrolled at Your School

POWERSCHOOL rights intentionally prevent the staff at one school from seeing information on students at another school, which complies with FERPA guidelines. The only exception is for MCPSS level personnel who have specific needs to see all school data and teachers or others who serve specific students in multiple schools.

It is important that staff members at one school do not attempt to give information about students enrolled in another school to individuals who ask for such information. Instead they should expect the person asking for the information to contact that school themselves. If the person asking for information does not know what school to contact, then they should be referred to the Student Services Department.

DO NOT tell an individual who has no official right to know where else the student is enrolled. Even if the person asking is a parent, there may be a dangerous situation that you are now unaware of, so the safe action to take is to refer such requests to the Student Services Department.

The danger in telling someone, employee or not, what other school the child is enrolled in lies in the fact that you have no access to that student's record and will not know if the child is in protective custody or is involved in some other situation such as custody dispute, etc. This could result in a safety issue.

This rule applies even when the person asking for the information is one of our own employees. Unless the person requesting the information is currently providing educational services to that student, they should not be given any information about them, including where the student is enrolled. And, if they are providing educational services to a student at another school, but claim not to know where the child is enrolled, then this should raise some flags. In this case, contact Student Services for guidance.

POWERSCHOOL Permission Standards for Mobile County Public School System

I. Permission Committee

(A) An POWERSCHOOL Permissions committee was formed in March of 2016, members include:

1) Technology Coordinator/Data Governance Committee chairperson
2) POWERSCHOOL Student Data manager and support staff responsible for POWERSCHOOL
3) Students Service department representatives
4) Principal representatives
5) Research Accountability Assessment Director

(B) Requests for changes to the standards set by the POWERSCHOOL Permissions committee can be made at any time by a school or MCPSS-level administrator. School administrators will be notified prior to the semi-annual committee meeting so that they can submit requests in writing prior to that date for consideration. Meetings will be held in January and July each year.

(C) Changes to settings may also be made by the committee decision as a result of software changes, new job roles, other local factors, directives from the State, or as determined by the Superintendent.

(D) The permissions are granted to individuals officially serving in the roles shown below. However, these permissions will not be granted automatically. The individual's principal/supervisor must endorse them by submitting their name to the Technology Department. In addition, these endorsements may be revoked if the principal, supervisor, or the committee determines that the access is no longer necessary or has other reasonable concerns. The POWERSCHOOL Permissions Committee makes the final determination for access settings.

(E) The POWERSCHOOL Permissions committee will meet semi-annually in order to review permissions and to consider new requests. Requests that are made between annual meetings will be presented to the members via email or in-person, as appropriate. Changes will be conveyed to affected personnel via memos and updates to the manual. (See Exhibit A.)

II. Allowable POWERSCHOOL Permission Settings

As of August 2014

Group: **Find Student Only** (Schedule Lookup)
Staff Affected: All POWERSCHOOL Users

All POWERSCHOOL users can use the Look Up feature to find any student's current location. The staff can also refer to a Student Schedule Matrix pdf file which the school's Registrar will post to the Faculty Share. Registrars will update the file as needed.

Only Technology POWERSCHOOL administrators can add individuals to this permission group.

Group: **Attendance**

Staff Affected: Assigned by Technology upon request

This level of permission allows the user to see the Summary, Main, and Contacts tabs.

It gives them the ability to check students in and out and to view the following information:

- Name
- Date of Birth
- Age
- Phone
- Gender
- Grade
- Address
- List of Contacts and their relationship and phone numbers

The user will see the special symbols, but not open up these notes to see what instructions they contain.

Only Technology POWERSCHOOL administrators can add individuals to this permission group.

Group: **Limited Student View**

Staff Affected: Library Media Specialists/Technology Support Teachers

Staff with "Limited Student View" permissions will have Read-Only rights to contact information for all students in the school.

**Library Media Specialist may have additional permissions if they give grades or serve in other roles within the school.*

Only Technology POWERSCHOOL administrators can add individuals to this permission group.

Group: **Special Student View**

Staff Affected: Individuals serving in the following roles, when endorsed by the principal/supervisor

- Athletic Directors (Can also be added to AD Quick Entry Edit Group, see below)
- Lead Special Ed Teachers
- Lead ESL Teachers
- PST Chairperson

Staff with "Special Student View" permissions will be able to see the following information for ALL students in the school:

- Contacts – full records

- Grades which have been posted by teacher
- Attendance profile
- Schedules

Principals may also want to ask Registrars to set up Non-Reporting Class Rosters (see below) for individuals who have been granted Special Student View permissions. Or, they may want to request that these individuals be set up with Non-Reporting Class Rosters *instead of* being given the Special Student View. In either case, Non-Reporting Classes can make it easier for individuals to look up information on the students they are responsible for because it will enable them to check each student's information from a 'class' roster (i.e. football, PST, girl athletes, etc.) rather than look up each student by name in POWERSCHOOL. Creating these 'Non-Reporting Class Rosters' will take more work on the Registrar's part. However, it is a good option when principals want to restrict access to only the students served by the individual, rather than all students in the school.

Group: **Athletic Directors**

Staff Affected: Athletic Directors only

Middle and high school athletic directors will be given the ability to use the Entry feature in POWERSCHOOL to edit students' eligibility settings, but only after being trained by the school registrar.

Athletic Directors with this permission must sign the associated Security Agreement.

Group: **Non-Reporting Class Rosters**

Staff Affected: **Various**

When teachers have a formal responsibility to support students who they do not have on a class roll, and this responsibility includes viewing the students' grades, then the Registrar may be asked to set up a Non-Reporting Class for that teacher. Examples of these situations/individuals include:

- Special Education teachers with students on their caseload, but who are not in their class
- Academics First Sponsor
- Math or Reading Coaches, where applicable
- Gifted advisors, where applicable
- Anyone who already has or would be eligible for the Special Student View (above)

Once the 'class' is created, the 'teacher' will have the ability to 'print' a comprehensive progress report for the students which will give the 'teacher' access to posted grades from all classes. Keep in mind that this will take some work on the Registrar's part. In the case of the Athletic Director and a separate Academics First teacher, they could both be listed as teachers for the non-reporting class to minimize the work involved.

The Technology Department will provide Registrars with directions for creating these non-reporting classes. These directions must be followed carefully so that the courses do not affect attendance, LEAPS, or other state reports. These courses will need to be scheduled outside of the school day, must be tagged as a non-reporting course in the Master Schedule, and must use the correct State Course Number.

Group: **Discipline History**

Staff Affected: Administrators Only

Only school administrators will have access to student discipline history. Staff should consult with their school administrators if they need discipline history on a given student.

AHSAA Student in Good Standing Forms –

The AHSAA Student in Good Standing Release Form must be completed and signed by the school Principal. This is only to be completed when the student athletes leaving your school are not in good standing.

I. POWERSCHOOL Substitute Teacher Set Up & Roles

As of August 2014

All Subs and Temporary Employees who are granted POWERSCHOOL access must sign the PowerSchool SiS Security Agreement. The school registrar should facilitate this and store the Agreement at the school. If a Long Term Sub works at more than one school, each school should have a signed Agreement on file.

When possible, the teacher going on leave should set up the class grade book before the Long Term Sub takes over. Technology POWERSCHOOL administrators can assist in setting up grade books if the teacher is not able to do so prior to his/her absence.

Group: **Substitute Teacher Access**
Staff Affected: Long Term Subs and Temporary Employees

Scenario 1: **Short Term Sub (under 21 days)**

POWERSCHOOL: No access

- If the teacher does not return after 20 days, then the sub may have POWERSCHOOL access as a Long Term Sub. Select the appropriate Scenario from those listed below.

- If it is known in advance that the teacher will be out for longer than 20 days but less than 1 semester then use either Scenario 2 or 3, whichever applies.

Scenario 2: Sub over 21 days, but less than 1 Semester (ie. Long Term Sub)

POWERSCHOOL Role: Long Term Sub
POWERSCHOOL Schedule: Additional Teacher

Scenario 3: Long Term Sub/Temporary Employee* for <u>more</u> than 1 semester, but <u>less</u> than 1 year

POWERSCHOOL Role: Long Term Sub
POWERSCHOOL Schedule: Additional Teacher

EXCEPTION: If the original teacher will <u>not</u> be returning to your school (i.e. transferring, resigning, retiring, etc.) then they should be removed from the master schedule and the teacher replacing them should be shown as:

POWERSCHOOL Role: Long Term Sub
POWERSCHOOL Schedule: Teacher

Scenario 4: Temporary Employee* for one full year

If the ***original teacher has highest degree*** and years of experience, then the Temporary
Employee will have:

POWERSCHOOL Role for Temporary Employee: Long Term Sub

POWERSCHOOL Schedule for Temporary Employee: Additional Teacher

POWERSCHOOL Role for Teacher on Leave: First Primary Teacher

POWERSCHOOL Schedule for Teacher on Leave: Teacher

If ***the temporary employee has highest degree*** and years of experience, then the Temporary Employee will have:

POWERSCHOOL Role:	First Primary Teacher
POWERSCHOOL Schedule:	Teacher
POWERSCHOOL Role for Teacher on Leave:	None
POWERSCHOOL Schedule for Teacher on Leave:	None

Email Use and Security Agreement

I. User Agreement

All individuals issued an email account by Mobile County Public School System are expected to follow MCPSS's Computer, Internet, and Electronic Communication Acceptable Use Policy. This policy is provided to all staff. (http://www.mcpss.com/email)

II. Mobile County Public School System Email Disclaimer

Adopted December 11, 2007

Any confidential e-mail, and/or files transmitted with it, is intended solely for the use of the individual or entity to whom it is addressed. The communication may contain material that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received an e-mail or communication in error, please notify the sender immediately.

Banking Security

I. ACH Transfers

The CFO should notify the Student Data Manager of any plans to change its electronic banking processes. The Technology Department will assist in evaluating whether or not any such practices would pose an unacceptable risk to MCPSS's network.

II. Bank Balance Auditing Recommendations for Preventing Electronic Theft

The Technology Department highly recommends that MCPSS and school bank balances which employ electronic payment measures, be checked daily, or within the timeframe given by the bank, in order to report fraudulent withdrawals in order to recover stolen funds.

Data Backup and Retention Procedures

I. Purpose of Data Backup and Retention Procedures

(A) Ensure that procedures for comprehensive data backup are in place and that system data is restorable in the event of data corruption, software or hardware failures, data damage or deletion (either accidental or deliberate), and properly executed requests from the office of the Superintendent, or forensic purposes.

(B) Provide a documented procedure of how long data is retained, and therefore restorable.

(C) Provide documentation of what systems and data are specifically included in, and excluded from, backup and retention.

(D) Establish the groups or individuals responsible for data backup and retention procedures, including the on-site and offsite locations of backup media.

(E) Establish the procedural guidelines used to initiate a data restore.

II. Scope

(A) These procedures apply to all servers and systems installed and controlled exclusively by the Mobile County Public School System Technology Department. (Systems Table I) and excludes servers and systems controlled by specific departments within Mobile County Public School System (Systems Table II). In cases where other Departments are responsible for their backup systems, the Technology Department will provide technical and professional guidance for backup routines and procedures, as requested.

(B) These procedures apply to all user data in the following manner:

All users with network permissions are trained and urged to store data onto their server workspace, but they are permitted to store files on local machines. Individuals users may delete their data from either network servers or local machines at will. If data stored on a server is deleted by the end user and falls outside of the backup period, the System has no method of recovering such files.

Files stored by users on individual hard drives or other individual storage devices are not backed up and may become unrecoverable in the case of hard drive failure or accidental deletion. Although technicians may be able to locate or recover locally stored files, these files are not part of the data backup or recovery plan.

(C) These procedures do not apply to connected systems which are the property, and therefore the responsibility, of outside entities such as the Alabama State Department of Education.

(D) These procedures include a special section for the e-mail and student data system, as its backup and retention systems are separate from other systems.

III. General System Data Backup Procedures

(A) Storage Area Network Fileshare Snapshots

1) As data is changed, replaced or deleted on school and MCPSS fileshares, older versions of that data are preserved.

2) Shadow Copy occurs automatically three times per day, Monday thru Friday.

3) Includes any data that has been added or modified in the last 10 days.

4) Shadow Copy versions are housed on the same device which originally contained the data.

5) Storage Area Network Devices are physically isolated and access is limited to protect systems from tampering and disturbance.

(B) Incremental Backups

1) System Data that has been added or modified since the last backup operation is backed up to centralized device.

2) Incremental Backups occur automatically once per day, 5 days a week. A Full Backup is performed once a week.

3) The centralized device is housed at the Network Operation Center (NOC), a facility designed for increased security and protection.

(C) Duplication of Backup Information

1) Backups are duplicated and are distributed to Disaster Recovery Servers located in two separate locations within the School System.

IV. E-mail Data Backup Procedures

(A) The e-mail system is a hybrid system, comprised of both on-premise and cloud-based servers.

(B) Two on-premise servers act as managers for mailboxes, with are located on cloud-based servers.

(C) The backup procedure is designed for a full-system restore, as well as the ability to restore individual messages.

(D) Backup processes are automatic.

V. Time Frames for Data Retention

(A) All statements of data retention, and the subsequent ability to restore that retained data, are subject to hardware and software components functioning properly.

(B) The time frames listed below are based on what time frames are currently possible and affordable with current staff and funds for backup servers and media. Time frames may change depending on the amount of data the System generates and the budget provided to manage these services. Time frame changes will be noted in a log kept by the System Technical Services Supervisor noting the reason for any time frame change and approval from the Deputy Superintendent.

(C) Data Retention timeframe is expressed as a minimal amount of time for which any protected data should be recoverable, utilizing the multiple protection mechanisms available under normal circumstances.

(D) In the event of a catastrophic event, such as the destruction of the Network Operations Center, some levels of data recovery will be affected, but recovery will still be possible to some point within the last 30 days provided off-site locations have not been similarly destroyed.

(E) Retention of General System Data.

1) Retained for normal restores for a period of one month.

(F) E-Mail Data is retained for a Disaster-Recovery full-system restore for a period of four weeks.

(G) Retention of Web Traffic and Browsing Data.

1) A log of sites visited by computer are retained for a period of 5 days.

(H) Backup logs will be maintained by Technology Personnel

(I) Litigation Holds

1) It shall be the responsibility of the Central Office administrators to promptly inform the Technology Department of any pending litigation where user files or emails may become part of eDiscovery requests.

2) Once notified, the Technology Department will take all available actions to retain all affected files and emails, such that they are not deleted according to the retention schedules above.

VI. Email Archiving

(A) As of March, 2020, board approved policy to retain a minimum of two years of e-mail was invoked. The size of the hard drive space allotted for this may need to be expanded over time to accommodate a full 2 years of data. Expansion of disk space will be based on available funding at the time.

VII. Data Included / Excluded

(A) Data is generally included by default when a new server or system is configured to be backed up by the centralized storage system.

(B) Configuration of the centralized storage system is reviewed twice per calendar year by the Network Administration Team (Network Engineers, Network Administrators and the Technical Services Supervisor) to ensure that systems are being adequately protected.

(C) All data included or excluded for the centralized storage system is included in (or excluded from all the routines of the system, including:

1) Server Shadows
2) Incremental Backups

(D) Data specifically included in the centralized storage system:

1) General application drives at schools
2) Faculty shared data areas
3) Student shared data areas
4) Backups repository on all servers

(E) Excluded data is generally excluded because it is especially large AND appears in the same format and version on multiple servers throughout MCPSS.

1) Data specifically Excluded from the centralized storage system:

a) Server Operating System, swap files, temp files & lock files.
b) Ghost files and ISO image files.
c) Uncompressed backup or transaction files
d) Static data that is replicated on multiple servers

VIII. Responsibility of Data Backup and Data Retention

(A) The Technology Department assumes responsibility of facilitating, operating, maintaining, checking and testing the centralized storage system.

(B) For schools leaving MCPSS, a backup copy of the POWERSCHOOL database will be turned over to PowerSchool after all state reports have been submitted and

approved by ALSDE at the end of the school year. It should be understood that the original data will remain with MCPSS.

(C) The chief architect and operator of the centralized storage system is Andy Berry.

(D) Andy Barry is responsible to provide documentation, and to instruct the members of the Network Administration and Network Technician groups, in the proper maintenance and operation of the centralized storage system.

(E) The ultimate responsibility of the centralized storage system, its maintenance, operation and procedures falls to (in order):

1) Andy Barry
2) Network Technicians

IX. Data Restore Procedures

(A) In the event that a network user requires that data be restored from the centralized storage system, they shall do one of the following:

1) Contact their School Technology Support Teacher (TST)
2) Contact the Technology Help Desk
3) Contact Andy Berry, Network Manager

(B) A MCPSS Technology work order shall be initiated for every requested restore, regardless of the outcome.

(C) Restores shall be given High Priority treatment and initiated in an expedited manner.

(D) The requestor shall be notified when the restore operations are complete, to ensure that data is accessible and meets the user's needs.

X. Systems Table I

Systems under the Control of the Technology Department

System	Location	Special Conditions	Date Changes/Notes
Web Server(s)	NOC		
School Domain Controller Servers	School NOC	Yes	

School Application Shares	School NOC	Yes	
Kronos	NOC		

XI. Systems Table II

Systems Assisted by the Technology Department

System	Location	Special Conditions	Date Changes/Notes
PCS	NOC		
Xerox	NOC		
Subfinder	NOC		
NextGen	NOC		

End of Document Backup and Retention Procedures

Alabama Data Breach Notification Act of 2018

The Board will comply with the three requirements of the Act for an entity:

1. Secure Sensitive Personally Identifying Information (SPII)
2. If a breach does occur, security coordinator will institute an investigation of the breach.
3. If a breach does occur, the board will notify those impacted by the breach.

Data Protection

I. Data Protected for Employees

Sensitive personally identifying information (SPII) is defined as a person's name (full name or first initial and last name) if it's combined with one of these:

(A) SSN or tax ID number;

(B) Driver's license number or other identifying number issued by the government;

(C) Bank account, credit card or debit card number if combined with a PIN, security code, password, or expiration date;

(D) Medical information;

(E) Health insurance policy number or identification number; or

(F) Username/email address if combined with password or security questions and answers.

II. Before a breach occurs, the board will maintain reasonable security measures and consider the following:

A. Designating an employee to coordinate security;
B. Identifying internal and external risks;
C. Adopting safeguards to address those risks and assess the effectiveness of those safeguards;
D. Evaluating and adjusting security measures to account for changes in circumstances;

and

E. Keeping management (including the board of education) informed of the entity's security status.

The reasonableness of an entity's security can consider the entity's size, the amount of SPII on hand, and the cost of implementing security measures.

III. What does the law require of a board after a breach?

If a breach is discovered, the security coordinator and the board must investigate the breach and notify those impacted.

The investigation will include the following:

A. An assessment of the nature and scope of the breach;
B. An identification of any SPII involved and what people have been impacted;
C. A determination of whether a wrongdoer has actually acquired SPII; and
D. Implementation of measure to restore security following the breach.

Written notice to those impacted by the breach must be given as soon as possible, but must be done within 45 days of the discovery. That notice must be delivered by mail or email and contain:

A. The date, estimated date, or date range of the breach;
B. A description of the SPII acquired;
C. A general description of what the entity has done to restore activity;

D. A general description of what the individual can do to protect themselves from identity theft; and
E. Contact information for the person they can contact about the breach.

If a third-party agent is breached, it must notify the covered entity of the breach within 10 days of its discovery. The entity may contract with the third party to provide required notices.

Exhibit A: - Identity Theft Training

Data Security Education for Registrars

Pending Board Approval

Operating a school and MCPSS means handling personal data for thousands of students and employees. It is our responsibility to take security measures to ensure that our data does not end up in the hands of identity thieves. According to the Federal Trade Commission's 2005 report:

- Alabama ranked 31st in reports of identity theft
- Birmingham, AL ranked highest in the number of victims
- The highest number of victims were in the 18-29 year old group

What is identity theft?

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Young people, 18-29 years of age, are the number one target for identity thieves, according to Quest, a communications company that is working to raise awareness of the issue.

Teenagers and young people are more vulnerable to identity theft than adults because most have not established credit records that can be monitored.

Teens also are more susceptible to identity theft because they are less likely to check their credit card records and may not even be aware of their credit record and its importance. Most teens have little or no knowledge of financial transactions and credit reports.

Most teens discover they have fallen victim to identity theft when they apply for a driver's license and are denied because one has already been issued under their Social Security number.

Source: **PBS Newshour**

How do identity thieves get your personal information?

- They get information from businesses or other institutions by:
  - *stealing records or information while they're on the job*
  - *bribing an employee who has access to these records*
  - *hacking these records*
  - *conning information out of employees*
- They may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.

- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."
- They may get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.
- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.
- They may steal your wallet or purse.
- They may complete a "change of address form" to divert your mail to another location.
- They may steal personal information they find in your home.
- They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or pretexting by phone.

What is "pretexting" and what does it have to do with identity theft?

Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. Pretexting is against the law.

Pretexters use a variety of tactics to get your personal information. For example, a pretexter may call, claim he's from a research firm, and ask you for your name, address, birth date, and social security number. When the pretexter has the information he wants, he uses it to call your financial institution. He pretends to be you or someone with authorized access to your account. He might claim that he's forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain other personal information about you such as your bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy. It is not pretexting for another person to collect this kind of information.

What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways.

Credit card fraud:

1. They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
2. They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:

- They may open a phone or wireless account, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:

- They may create counterfeit checks using your name of account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic transfers in your name, draining your accounts.
- They may take out a loan in your name.

Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

What do you do if you believe personal data has been exposed or stolen at your school site?

Notify both the Technology Coordinator and the Deputy Superintendent immediately. These individuals will take the appropriate next steps of investigating and notifying law enforcement.

Preventative Measures to be taken at all Mobile County School locations:

Ensure only authorized personnel have access to **POWERSCHOOL** and other applications that contain personal information.

- Use good password protection and do not give others access to your password or computer if you have access to software containing personal information.
- Do not use social security numbers on printed documents unless absolutely necessary.
- Shred any printed documents with personal information that was printed and is no longer needed.
- BE SURE ALL EMPLOYEES "Lock" or Log Off their workstations when away from their desks. (See instructions below).
- Educate your staff about identify theft.
- Ensure your employees are not giving out phone numbers or other personal information about employees or students to anyone who is not requesting it for an official business purpose. (Do not allow employees to give out the home phone numbers of parents or employees as a courtesy to someone who asks for it.)

Locking a computer workstation:
Press Control – Alt – Delete
Click "Lock Workstation"
When you return you will press any key and then use your password to log back into the computer.

Exhibit B: Computer, Internet, and Electronic Communication Acceptable Use

3.50

COMPUTER, INTERNET, AND ELECTRONIC COMMUNICATION ACCEPTABLE USE

MCPSS relies on its computer network to conduct its business. To ensure that MCPSS Computer Resources are used properly by its employees, students, independent contractors, agents, vendors, and other computer Users (the "Users"), the Board of School Commissioners for MCPSS has created and passed this Computer Use Policy (the "Policy"). The rules and obligations described in this Policy apply to all Users (the "Users") of MCPSS' computer network or Computer Resources, wherever they may be located.

MCPSS' policies against discrimination and harassment (sexual or otherwise) apply fully to MCPSS' Computer Resources and Resources, and any violation of those policies is grounds for discipline up to and including termination. Students who violate these policies are subject to disciplinary action consistent with Board policy and the Student Handbook. Vendors, consultants and other third parties must adhere to these policies and are subject to losing their right to access MCPSS Computer Resources for violations of these policies.

The term *Computer Resources* as used herein refers to MCPSS' entire computer, electronic and communications network. Specifically, the term *Computer Resources* includes, but is not limited to: computers, host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, tablets such as IPAD's, telephones, facsimile machines, scanners, software, data files, peripherals such as printers, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, e-mail systems) that may be accessed directly or indirectly (including access by Students, vendors, consultants and other third parties using personally owned computer hardware as authorized by MCPSS) from our computer network or that are owned or have been purchased by MCPSS.

The Computer Resources are the property of MCPSS and may be used only for legitimate business and educational purposes. Users are permitted access to the Computer Resources to assist them in the performance of their jobs. Computer and internet access is provided for MCPSS business *use,* but *occasional* minimal personal use is allowed. Use of the Computer Resources is a privilege that may be revoked at any time. Users who violate this Policy may have their Computer/Internet use privileges revoked at any time and without prior notice AND are subject to discipline up to and including the possibility of termination.

In using or accessing the Computer Resources, Users must comply with and be aware of the following provisions:

No Expectation of Privacy. The computers and computer accounts given to Users are to assist them in the performance of their jobs or in the case of students, in their educational studies and activities. Users should not have an expectation of privacy in anything they create, store, send or receive on the Computer Resources. Computer Resources belong to MCPSS and may be used only for the purposes set forth herein. MCPSS has the right, but not the duty, for any reason and without the permission of any User, to monitor any and all of the aspects of its Computer Resources, including, without limitation, reviewing documents created and stored on its Computer Resources, deleting any matter stored in its system, monitoring sites visited by Users on the Internet, monitoring chat and news groups, reviewing material downloaded or uploaded by Users from the Internet, and reviewing E-Mail sent and received by Users. Employees and Users should not have an expectation of privacy in anything they create, store, send or receive using the Computer Resources.

Waiver of privacy rights. MCPSS reserves the right to inspect the contents of all electronic data stored on MCPSS computer equipment or Computer Resources. Users, in using MCPSS Computer Resources, expressly waive any right of privacy in anything they create, store, send or receive on MCPSS Computer Resources or through the Internet or any other computer network. Users consent to allowing personnel of MCPSS to access and review all materials Users create, store, send or receive on the computer or through the Internet or any other computer network. Users understand that MCPSS may use human or automated means to monitor use of its Computer Resources, including data stored on the local drive, data stored on any network drive, and electronic mail.

Passwords. Users are responsible for safeguarding their passwords for access to the Computer Resources or Computer Resources. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made and actions taken using their passwords. No User may access the Computer Resources with another User's password or account. Use of passwords to gain access to the Computer Resources or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the Computer Resources.

Viruses and Virus Protection. Users may not disable or remove virus protection software. Viruses can cause substantial damage to Computer Resources. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into MCPSS' Computer Resources or computer network. Virus software updates are automatically distributed regularly to Computer Resources. Users may not interrupt the update process and must report any errors in the update process immediately to MCPSS' support help desk. PCs not attached to the LAN must be updated by the User. The Information Technology Department will provide virus updates.

Compliance with applicable laws and licenses. In their use of Computer Resources, Users must comply with all software licenses, copyrights and all other state, federal and international laws governing intellectual property and online activities. It is **MCPSS'** policy to comply fully with all software copyright licenses. Employees who willfully circumvent this policy will be subject to disciplinary action up to and including termination of employment. In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

Prohibited Activities. The following activities, items or materials are prohibited:

Inappropriate or unlawful material. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups), downloaded from the Internet or displayed on or stored in MCPSS computers. This includes e-mails known as "Spam" and e-mails containing nonbusiness related matters. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

Without prior written permission from the Executive Manager of Information Technology. Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material or any other unauthorized use, including material or significant personal uses.

Using or copying software in violation of a license agreement or copyright. Violating any state, federal or international law.

Waste of Computer Resources. Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

Accessing other User's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. The ability to read,

alter or copy a file belonging to another User does not imply permission to read, alter or copy that file. Users may not use the Computer Resources to "snoop" or pry into the affairs of other Users by unnecessarily reviewing their files and e-mail. Excepted from this provision are those persons conducting investigations or administrative duties at the request and with the authorization of the Executive Manager of Information Technology or Executive Manager of Human Resources.

Misuse of software. Without prior written authorization from the Executive Manager of the Information Technology Department, Users may not do any of the following:

(1) Copy software for use on their home computers;
(2) provide copies of software to any independent contractors or third party;
(3) install software on any MCPSS workstations or servers;
(4) download any software from the Internet or any other online service to any MCPSS workstations or servers;
(5) modify, revise, transform, recast, or adapt any software or reverse-engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors; and
(6) Users who have copied software for home computers, distributed software or installed software on corporate computers must obtain approval according to the current guidelines or remove the software immediately.

If you become aware of someone using Computer Resources for any of these activities, you are obligated to report the incident immediately to your supervisor. Violations of any aspect of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

E-Mail Policy

To maximize the benefits of its Computer Resources and minimize potential liability, MCPSS has created this E-mail usage policy. All computer Users are obligated to use these resources responsibly, professionally, ethically, and lawfully.

Employees and other Users are given access to our computer network to assist them in performing their duties. Employees and Users, including students, should not have an expectation of privacy in anything you create, store, send or receive on the Computer Resources. The Computer Resources belong to MCPSS and may only be used for business purposes. Without prior notice, MCPSS may review any material created, stored, sent, or received on its network or through the Internet or any other computer network**.**

Sending unsolicited e-mail (spamming). Without the express permission of their supervisors, employees may not send unsolicited e-mail to persons with whom they do not have a prior relationship.

Altering attribution information. Employees must not alter the "From:" line or other attribution-of-origin information in e-mail, messages, or postings. Anonymous or pseudonymous electronic communications are forbidden. Employees must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, sending e-mail, or otherwise communicating online.

Attorney-client communications. E-mail sent to in-house counsel, if any, or an attorney representing MCPSS should include this warning header on each page: "ATTORNEY-CLIENT PRIVILEGED; DO NOT FORWARD WITHOUT PERMISSION." Communications from attorneys may not be forwarded without the sender's express permission.

Confidential Transmissions. Any confidential e-mail, and/or files transmitted with it, is intended solely for the use of the individual or entity to whom it is addressed. The communication may contain material that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received an e-mail or communication in error, please notify the sender immediately.

Internet Use Policy

The Internet can be a valuable source of information and research. In addition, e-mail can provide an excellent means of communicating with other employees, our customers, and clients, outside vendors and other businesses. Use of the Internet, however, must be tempered with common sense and good judgment. Users who abuse their use of Computer Resources to access the Internet may have access to the Internet restricted or removed. In addition, Users who violate this policy may be subject to disciplinary action, including the possibility of termination, student discipline (as applicable) and civil and criminal liability.

Your use of the Internet is governed by this policy:

Disclaimer of liability for use on Internet. MCPSS is not responsible for material viewed or downloaded by Users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

Employees' duty of care. Employees should endeavor to make each electronic communication truthful and accurate. You should use the same care in drafting e-mail / electronic documents as you would for any other written communication. Please keep in mind that anything created or stored on the Computer Resources may, and likely will, be reviewed by others.

Duty not to waste Computer Resources. Because audio, video and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related***.***

No privacy in communications. Users of MCPSS Computer Resources should never consider electronic communications to be either private or secure. E-mail may be stored indefinitely on any number of computers, including that of the recipient. Copies of your messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect usernames may be delivered to persons whom you never intended.

Monitoring of computer usage. MCPSS has the right, but not the duty, to monitor any and all aspects of its Computer Resources, including, but not limited to, monitoring sites visited by Users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by Users to the Internet and reviewing e-mail sent and received by Users.

Blocking of inappropriate content. MCPSS may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by MCPSS networks. In the event you, nonetheless, encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to MCPSS blocking software.

Games and entertainment software. Users may not use MCPSS' Internet connection to play games, download games or other entertainment software including screen savers. Educational games approved by the teacher and or administration of the MCPSS are exempt from this provision.

Illegal copying. Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy.

Accessing the Internet. To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to MCPSS' network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited.

Prohibited Activities. The prohibited activities referenced above are also prohibited in connection with Users of MCPSS' Computer Resources use of the internet. Users must avoid internet websites and locations that are ***harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate while using MCPSS Computer Resources.***

Students

The board supports access by students to rich information resources and the development by staff of appropriate skills to analyze and evaluate such resources.

All such materials shall be consistent with board-system guidelines and staff will provide guidance and instruction to students in the appropriate use of such resources.

Annually, students and parents will be given MCPSS' guidelines and rules governing procedures for acceptable use of the Internet describing the information available and prohibited uses of system computers. Students and parents must sign a written statement acknowledging the guidelines for them to access the Internet at school.

In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. In compliance with federal law, the online activities of minors **will** be monitored.

Employees

Employees will be provided with a copy of the MCPSS acceptable use guidelines and sign a statement that they agree to the terms.

See also Board Policy 6.12

References – Procedures: *Computer,* Internet*, and Electronic Communication* Acceptable Use

Date Adopted: December 11, 2007

Public Hearings: March 19, 2013, March 25, 2013

Amended: March 23, 2011, March 25, 2013

Exhibit C: Copier Machine Security Recommendations

July 2011

Many modern copy machines and multifunction printers record images of all information being copied, faxed, or scanned onto their hard drives. In the case of the Sharp multifunction machines, an image of every print job, fax, and copy ever made on the machine is retained on its hard drive. In our environment, these images could include FERPA- protected educational records, Social Security numbers, I.E.P.s, and other confidential information. Schools need to be aware that there have been instances where criminals have data-mining copy machine hard drives either disposed of in landfills or taken from previously leased machines.

School administrators should take measures to ensure that the hard drives on any copier or multifunction machine their school uses is properly erased or disposed of when the use of the machine is terminated.

Leases –

Ask the vendor what data protection options are available prior to signing a contract. Add an appropriate option to the contract and be sure to require a Letter of Certification once the machine is returned to the dealer.

Purchases -

Find out if the machine is equipped with data security technology already embedded into it and what this entails.

Enter a ticket for the Technology Department to remove and dispose of the copy machine hard drive prior to sending it to the local landfill or putting it out for auction.

Provisions for Consideration – Not Yet Implemented

Electronic Signature Agreement (Not Implemented)

[The following proposed agreement does not directly impact data security. But it could impact the outcome of challenges in cases where staff were asked to sign user agreements containing rules regarding data security electronically, but later protest that their digital signature was not valid.]

Mobile County Public School System uses many types of electronic communications in order to conduct business. These include electronic mail, documents, applications, and forms. Digital formats enable MCPSS to transmit information rapidly and to and retain records efficiently. Throughout your employment with Mobile County Public School System you will have occasion to use these various methods to make and respond to requests, convey and receive information, and electronically 'sign' forms and agreements.

> The Uniform Electronic Transactions Act (UETA) provides a legal framework for the use of electronic signatures and records in government or business transactions. UETA makes electronic records and signatures as legal as paper and manually signed signatures. This Act was adopted by Alabama in 2001 (Ala. Code §8-1A-1 et seq.) It defines an electronic signature as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

Mobile County Public School System may use a variety of methods to verify your electronic 'signature' or identity. These include: 1) submitting a form while logged into the network or software application under a password protected account and 2) submitting your employee id or social security number within a form along with other personal information that uniquely identifies you. Therefore, you must keep your network and software login ids and passwords secure at all times.

Agreement

I agree to maintain the security of the UserID and password assigned to me by Mobile County Public School System in order to prevent disclosure of this information to anyone.

I agree that, if I have any reason to believe that the security of my UserID and password has been compromised, I will immediately inform the helpdesk.

I agree that I will be held legally bound, obligated, and responsible for any submission I make in electronic format to Mobile County Public School System as I would be by making such submission in hardcopy form with my handwritten signature as certification.

I understand that if I decline to use an electronic 'signature' for any particular communication or form, that I may be required to submit that form in a hardcopy form with a handwritten signature; and that is it my responsibility to inform the appropriate person that I am taking this action.

I understand that if there is a hardcopy versions and an electronic version of the same exact document, that the one that is most recent will be considered the binding document and that the handwritten document alone may not override the electronic version.

References:

Section 8-1A-13 - Admissibility in evidence.

(a) In any proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

(b) In determining the attribution and authenticity or evidentiary weight of an electronic record or signature, the trier of fact may consider, along with any other relevant and probative evidence, proof of the efficacy of any security procedure applied. This may include a showing that the procedure: (1) uniquely identifies the signer or creator of the record; (2) prevents others from using the same identifier; and/or (3) provides a mechanism for determining whether the data contained in the record was changed after it was created or signed. Evidence bearing on the means and the reliability with which the procedure performs these functions may also be considered.

Section 8-1A-5 - Use of electronic records and electronic signatures; variation by agreement.

(a) This chapter does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(b) This chapter applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

(d) Except as otherwise provided in this chapter, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words "unless otherwise agreed," or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable law.

Restrictions on Parents Posting Images of Students (who are not their own children) to Social Media (Not Implemented)

From correspondence with a school in response to their question about a parent who wanted to post school pictures to Social Media.

With respect to pictures of students being posted online on sites that are not on our servers, we are trying to prohibit this for our staff and discouraging it for parents. The number of complaints we have been getting because a parent will take pictures of children who are not theirs and post them online has risen sharply in the last two years. For this reason we have tried to support our schools in discouraging parents from posting pictures of other children on the web. Coming to school is different than joining a little league team or some other voluntary activity. We don't think the classroom teacher or the school could give an individual the right to post pictures of his/her class online without having control of the site and ensuring that every other parent has agreed to this and has access. From our district's standpoint, we think all material posted online about school should be on our servers or a server which we have control over and administrative access to.

SCHOOL VOLUNTEERS

Volunteers, parents and other community members with approval of the local school principal can assist schools in many capacities.

Volunteers may be permitted to perform non-instructional tasks without direct supervision but should not have unsupervised access to children.

The Mobile County Public School System shall also comply with all laws (and amendments thereto) concerning adult sex offenders.

Legal Reference: Ala. Code § 15-20A-17 (as amended by Act 2014-421)

Date Adopted: December 11, 2007
Date Amended: October 27, 2015

FUNDRAISING

All school-based fundraising projects must be approved by the school principal. Any system-wide fundraising effort must be approved by the superintendent. Any fundraising effort on behalf of the school system must be approved by the superintendent.

Groups or their sponsors should be required to submit a fundraiser request and a fundraiser budget for any planned event. When deciding on fundraiser projects such things as purpose, need, potential profitability, and available volunteers should be considered. The health, safety, and welfare of students, parents, and the general public should be a primary consideration.

Date Adopted: December 11, 2007

ASSOCIATIONS/COLLECTIVES

The board recognizes the potential benefits to public education of the pursuit of excellence through membership in associations and organizations with goals consistent with those of the board. The board authorizes the superintendent to approve memberships deemed to be in the best interests of the school system and public education.

Date Adopted: December 11, 2007

SCHOOL FACILITY USE

The superintendent or his designee will approve in advance and in writing all special programs sponsored by individuals and groups that are not affiliated with the school, school board or a school group if a charge is to be made for admission or if a collection is to be taken at the end of the performance or activity.

Rentals and Service Charge

Any fees collected for the temporary use of school facilities shall be forwarded to the Facilities Division attached with the approved School Use of Facilities form. All funds received shall be forwarded to the Chief Financial Officer and deposited into the General Operation account for system-wide operating expenses.

Date Adopted: December 11, 2007

FLAG DISPLAYS

Reference: Alabama Code - §16-43-1.

Date Adopted: December 11, 2007