



Our Mission Statement

Equip every young child and family for success.

FULL COALITION BOARD PACKET **REVISED** October 22, 2026 – 8:30 a.m.

I. Call to Order

T. Panzer

II. Roll Call

B. Montalvo

III. Ratification

- *Budget for FY 2026 – 2027 R-2
- *IT Policy for FY 2026 – 2027 R-1

M. Easter

M. Easter

IV. Action

- Full Coalition Board Meeting Minutes:
 - August 27, 2026
- Financials
 - ** July 2026
 - **August 2026**
- **Revised Fiscal Policy – Cash Management
- Org Chart for 2026 – 2027 R-1 as of 10/22/2026

L. Sims / T. Panzer

Z. Hackley

Z. Hackley

M. Easter

L. Sims

V. Information

- CEO Updates
- Give4Marion Results Update
- 2025-2026 Community Annual Impact Report

L. Sims

W. Williams

W. Williams

VI. Community Roundtable Updates

VII. Upcoming Meetings

- Executive Committee Meeting – ELCMC – Thursday, November 12, 2026 – 8:30 AM
- Executive Committee / Full Coalition Board Meeting – ELCMC – Thursday, December 10, 2026 – 8:30 AM

VIII. Public Comment

IX. Adjournment

*Initial **action** completed through the Executive Committee

Initial **motion completed through the Executive Committee

Ratification Items



Ratification Sheet

FULL COALITION BOARD

October 22, 2026

SUBJECT: 2026 – 2027 ELCMC Proposed Budget Revision 2

Fiscal Impact: Total Revenue \$212,765

RATIFICATION

Ratify the 2026 – 2027 ELCMC Proposed Line-Item Budget Revision 2.

BACKGROUND INFORMATION

Revisions in the budget include changes from the Division of Early Learning's (DEL) Notice of Award (NOA) Revision 2 & 3, effective September 3, 2026.

Revenue	
RII – SR Plus Revert and Reappropriate	\$101,248
RII – Special Needs Differential Allocation	\$4,348
RIII – July Special Invoice R/R Allocation	\$107,169

Expense	
SR Direct Service	\$112,231
Special Needs	\$4,348
SR Plus	\$96,186

On September 10, 2026, the Executive Committee approved the 2026 – 2027 ELCMC Proposed Line-Item Budget Revision-2 as stated above.

Supporting Documentation Included:

- 2026 – 2027 ELCMC proposed budget R-2

R-1 8/6/2026											R-2																							
Approved Budget											Proposed Budget																							
2026-27											2026-27																							
Revenues											Notes																							
4001	Grants: State	\$	22,505,050	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	22,717,815															
100	FOEL: School Readiness	\$	16,828,285	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	17,041,050															
	* Direct Service	\$	12,475,957	\$	82,635	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	12,558,592															
	* Administration	\$	828,748	\$	5,576	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	834,324															
	* Non-Direct	\$	2,154,744	\$	14,497	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	2,169,241															
	* Quality	\$	662,998	\$	4,461	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	667,459	Align to DEL Allocation R1&R2														
	* Gold Seal	\$	301,957	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	301,957															
	* Special Needs	\$	6,690	\$	4,348	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	11,038															
	* Match	\$	143,860	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	143,860															
	* QPI Differentials	\$	253,331	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	253,331															
	* SR Plus	\$	-	\$	101,248	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	101,248															
	* SR Waitlist	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	Align to DEL Allocation R1&R2														
110	FOEL: Voluntary Pre-kindergarten	\$	5,527,521	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	5,527,521															
	* Direct Service	\$	5,264,306	\$	- <td>\$</td> <td>-</td> <td>\$</td> <td>-</td> <td>\$</td> <td>-</td> <td>\$</td> <td>-</td> <td>\$</td> <td>-</td> <td>\$</td> <td>-</td> <td>\$</td> <td>5,264,306</td> <td></td>	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	5,264,306															
	* Administration	\$	263,215	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	263,215															
	* VPK Assessment	\$	27,337	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	27,337															
130	CF: Help Me Grow	\$	121,907	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	121,907															
4010	Grants: Local Government	\$	180,000	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	180,000															
4020	Grants: Other	\$	1,000	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	1,000															
4050	Gifts, Donations, and Pledges	\$	32,060	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	32,060															
Multiple	Investment Earnings	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-															
Multiple	Other Miscellaneous Revenue	\$	2,000	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	2,000															
Total Revenue		\$	22,720,110	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	22,932,875															
Expenditures																																		
Capital Expenditures											\$	-	\$	-	\$	-	\$	-	\$	-	\$	-												
Employer Provided Salaries and Benefits											\$	3,061,314	\$	2,684,388	\$	256,598	\$	116,123	\$	-	\$	3,205	\$	1,000	\$	3,061,314								
Staff Development											\$	7,500	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	7,500								
Professional Services											\$	171,340	\$	161,889	\$	9,451	\$	-	\$	-	\$	-	\$	-	\$	171,340								
Direct Services - Child Care											\$	18,738,328	\$	13,510,002	\$	5,264,306	\$	-	\$	150,000	\$	26,785	\$	-	\$	18,951,093								
6500	Direct Services	\$	13,324,022	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	26,785	\$	-													
100	* School Readiness	\$	12,618,184	\$	112,231	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	26,785	\$	-													
100	* Match	\$	143,860	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
100	* QPI Differentials	\$	253,331	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
100	* Gold Seal	\$	301,957	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
100	* Special Needs	\$	6,690	\$	4,348	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
100	* SR Plus	\$	-	\$	96,186	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
110	* Voluntary Pre-kindergarten	\$	5,264,306	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
410	* Marion County (Match)	\$	150,000	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-													
Occupancy											\$	81,720	\$	75,182	\$	6,538	\$	-	\$	-	\$	-	\$	81,720										
Postage, Freight, and Delivery											\$	1,000	\$	920	\$	80	\$	-	\$	-	\$	-	\$	-	\$	1,000								
Equipment Leases											\$	5,040	\$	4,637	\$	403	\$	-	\$	-	\$	-	\$	-	\$	-	\$	5,040						
Supplies											\$	25,412	\$	23,489	\$	1,923	\$	-	\$	-	\$	-	\$	-	\$	-	\$	25,412						
Communications											\$	18,960	\$	17,443	\$	1,517	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	18,960				
Insurance											\$	51,033	\$	48,824	\$	1,967	\$	232	\$	-	\$	10	\$	-	\$	-	\$	-	\$	51,033				
Tangible Personal Property											\$	70,000	\$	64,400	\$	5,600	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	70,000				
Quality Initiatives											\$	251,612	\$	225,000	\$	-	\$	3,552	\$	-	\$	-	\$	23,060	\$	-	\$	-	\$	251,612				
Travel											\$	21,000	\$	19,000	\$	-	\$	2,000	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	21,000		
Other Expenses											\$	61,500	\$	55,024	\$	6,476	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	61,500		
Other Program Expenses											\$	154,350	\$	143,350	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	154,350
Depreciation											\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-
Total Expenditures		\$	22,720,109	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	22,932,874															
Total Revenue		\$	22,720,110	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	22,932,875															
Total Expenditures		\$	22,720,110	\$	212,765	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	22,932,875															
Net Proceeds		\$	(0)	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	-	\$	(0)															



Ratification Sheet

FULL COALITION BOARD

October 22, 2026

SUBJECT: FY 2026 – 2027 IT Policy – Revision 1

Fiscal Impact: N/A

RATIFICATION

Ratify the revised IT Policy to incorporate the cybersecurity requirements requested by the Division of Early Learning (DEL) on August 14, 2026, including alignment with Chapter 60GG-2, Florida Administrative Code. The revisions strengthen cybersecurity governance, risk management, access controls, monitoring, incident response, personnel security, system protection, and documentation requirements, while establishing specific review and compliance timeframes.

Additionally, approve the new IT100.07 – Electronic Records and Electronic Signatures policy, developed in response to a control identified during the Coalition’s preparation for fiscal monitoring. The new policy establishes requirements for the use, security, integrity, authenticity, verification, auditability, and retention of electronic records and electronic signatures used to conduct, document, approve, and retain official Coalition business transactions.

BACKGROUND INFORMATION

The Early Learning Coalition of Marion County adopted a comprehensive Information Technology Policy Manual on June 25, 2026, effective July 1, 2026. The policy was developed to modernize the Coalition’s technology governance framework and address the evolving technology environment, including cloud systems, remote work, mobile devices, data privacy, artificial intelligence, cybersecurity, and regulatory requirements.

Following implementation of the revised policy, the **Division of Early Learning (DEL) requested additional revisions on August 14, 2026, to further align the Coalition’s Information Technology Policy with current cybersecurity and regulatory expectations, including the requirements and framework established under Chapter 60GG-2, Florida Administrative Code. The requested revisions are due back to DEL no later than September 14, 2026.

The requested revisions strengthen the Coalition’s existing policy by adding requirements related to cybersecurity risk assessment and management, continuous security monitoring, incident classification and response, access controls, multifactor authentication, personnel security, vulnerability and patch management, documentation, and ongoing policy and system reviews.

During the Coalition’s preparation for fiscal monitoring, management also identified the need for a formal policy governing electronic records and electronic signatures. The existing IT Policy did not specifically address the controls necessary to ensure electronic signatures are unique to the signer, maintained under the signer’s control, capable of verification, and linked to the associated electronic record in a manner that protects the integrity and auditability of the transaction.



Management has therefore added IT100.07 – Electronic Records and Electronic Signatures to establish written controls for electronic records and electronic signatures and to address applicable federal and state requirements, funding and contractual requirements, and internal control expectations.

Management has incorporated the requested revisions into the Information Technology Policy Manual to ensure the Coalition’s technology governance framework remains current, adequately documented, and aligned with applicable cybersecurity, contractual, grant, and regulatory requirements.

On September 10, 2026, the Executive Committee approved the IT Policy for 2026 – 2027 Revision 1 as stated above.

Supporting Documentation Included:

- FY 2026 – 2027 IT Policy R-1



Page 3 & 4

- **New section added:** Adds a dedicated “60GG-2 Alignment and Gap Closure” section that was not included in the original policy.

Page 4

- **Authorization requirement:** Changes “may authorize” to “shall authorize,” making Executive Leadership authorization a required step rather than a discretionary action.

Page 6

- **Monitoring authority:** Changes “may monitor, access, and audit” to “shall monitor, access, and audit,” making monitoring, access, and auditing a required organizational authority rather than discretionary.

Page 7

- **Review frequency:** Changes from a general/periodic review to a requirement to review the policy **at least annually** and after material changes.
- **Review triggers:** Specifically adds material changes to operations, technology, applicable laws, grant obligations, contractual requirements, and cybersecurity standards as triggers for review.
- **Policy revisions:** Changes “may be made” to “shall be made as needed,” making updates a requirement rather than discretionary.
- **Supporting documents:** Changes “may issue” supporting standards, procedures, and guidance to “shall issue” them as necessary.
- **Removed language:** The revised section removes the provision stating that the more restrictive law, regulation, grant requirement, or contractual obligation controls in the event of a conflict.

Page 8

- **New section added:** Adds a dedicated “Cybersecurity Risk Assessment and Risk Management” section that was not included in the original policy.

Page 9

- **Specific timeframe added:** Changes “promptly” to a defined requirement of **within five (5) business days of notification** of a job role, responsibility, or employment status change.
- **Immediate action clarified:** Adds an exception requiring access to be updated **sooner when elevated risk or separation requires immediate action**.
- **MFA requirements strengthened:** Changes from requiring MFA “where technically feasible and implemented” to specifically requiring MFA for:
 - Remote access
 - Privileged accounts
 - Systems containing confidential, restricted, financial, personnel, or programmatic data
- **Technical limitations documented:** Adds a requirement that any inability to implement MFA due to a technical limitation must be documented through the exception and risk acceptance process.
- **Review frequency established:** Changes from “periodic” reviews to **at least quarterly reviews** for systems containing confidential, restricted, financial, personnel, or programmatic data.
- **Personnel changes addressed:** Adds a specific requirement to conduct a user access review **within five (5) business days of notice of a material personnel status change**.



- **Scope clarified:** The quarterly review requirement specifically applies to systems containing **sensitive or critical Coalition data**.

Page 10

- **Timing requirement strengthened:** Removes “as soon as practicable” and establishes a specific deadline of **no later than the individual’s final working day**.
- **Immediate termination of access:** Adds a requirement for access to be disabled **immediately upon notification** of:
 - Involuntary separation
 - Elevated security risk
 - Revoked authorization
- **Alternate timeframe strengthened:** Changes the requirement for an alternate timeframe to be **formally approved and documented** and adds that it must be **supported by compensating controls**.
- **Technical feasibility removed:** Removes “Where technically feasible,” making audit logging a standard requirement rather than conditional on technical capability.
- **Logging requirement strengthened:** Establishes that systems containing confidential, financial, personnel, or programmatic information **shall maintain sufficient audit logs**.
- **Exception process added:** Requires systems that cannot support the required logging to be **documented through the exception and risk acceptance process**.

Page 10 – 12

- **New section added:** Adds a **60GG-2 Cybersecurity Alignment and Control Matrix** to the policy.

Page 12

- **Critical updates clarified:** Changes “may be required immediately” to “**shall be required immediately when necessary to address significant security risk**.”
- **Monitoring requirement strengthened:** Changes “may be monitored” to “**shall be monitored**,” making system monitoring for security, compliance, and operational purposes mandatory.
- **Logging requirement strengthened:** Changes “may be logged, reviewed, and audited” to “**shall be logged, reviewed, and audited**,” establishing a required process rather than a discretionary one.

Page 12 & 13

- **New section added:** Adds specific requirements for **security continuous monitoring and detection** that were not previously addressed in this section.

Page 13

- **Reporting deadline added:** Requires suspected incidents to be reported **immediately and no later than 24 hours after discovery**, establishing a specific reporting timeframe.
- **IT responsibility strengthened:** Changes IT “will assess” to “**shall assess**,” making incident assessment a required responsibility.
- **Severity documentation added:** Requires IT to **assign a severity level and document the determination**, creating a formal record of incident classification.



- **Scope of documentation expanded:** Changes “where appropriate” to a mandatory requirement for **all confirmed security incidents** and suspected incidents involving confidential, restricted, financial, personnel, or programmatic data.
- **Evidence preservation clarified:** Requires the Coalition to preserve **relevant evidence** as part of the incident response process.

Page 13 & 14

- **New section added:** Adds specific requirements for **incident classification, reporting, escalation, and lessons learned** that were not previously addressed in this detail.

Page 14

- **Split tunneling requirement strengthened:** Changes from “may be restricted or prohibited based on risk level” to a clear prohibition: **split tunneling is prohibited unless explicitly approved by the CAO or Designee.**
- **Business justification added:** Any exception must be supported by a **documented business need.**
- **Formal risk review added:** Exceptions must go through the **exception and risk acceptance process.**
- **Remote access requirement strengthened:** Changes “may access” to “shall access,” making use of Coalition-approved or managed devices a mandatory requirement.
- **BYOD exception added:** Creates an exception allowing **Bring Your Own Device (BYOD)** access when formally approved by the **CAO or Designee.**
- **Security controls required for BYOD:** Requires approved BYOD exceptions to have **documented approval and required security controls** in place.
- **Conditional language removed:** Removes “if applicable to your environment,” making the device requirement more definitive.
- **Monitoring requirement strengthened:** Changes “may be logged, monitored, and audited” to “shall be logged, monitored, and audited,” making monitoring and auditing mandatory.
- **Response to suspicious activity expanded:** Changes from suspicious or unauthorized activity potentially resulting in immediate termination to requiring the activity to be **reviewed and documented by IT or the CAO/Designee.**
- **Suspension option added:** Adds **immediate suspension** as an option before termination when necessary to protect Coalition systems or data.
- **Authority and criteria clarified:** Establishes that access may be suspended or terminated when **necessary to protect Coalition systems or data**, providing a clearer basis for action.

Page 15

- **Frequency requirement added:** Changes from “may conduct periodic” awareness activities to requiring **at least one cybersecurity awareness activity each quarter.**
- **Discretionary language strengthened:** Changes “may conduct” to “shall conduct,” making ongoing cybersecurity awareness activities mandatory.
- **Examples consolidated:** The updated language combines the examples into one sentence describing acceptable quarterly activities, while retaining the same types of activities.

Page 16



- **Screening requirement strengthened:** Changes “may conduct” to “shall conduct,” making personnel screening a required process when applicable.
- **When screening is required clarified:** The updated language specifies that screening is required when based on **applicable laws, regulations, funding requirements, position responsibilities, or organizational policy.**
- **Position responsibilities added:** Adds **position responsibilities** as a factor in determining whether screening is required.
- **Documentation requirement added:** Changes “may vary based on” to “**shall be determined and documented based on,**” requiring the Coalition to document the basis for its screening requirements.
- **Requirement strengthened:** Changes “may be required” to “**shall be required,**” making confidentiality agreements, acceptable use acknowledgments, security awareness acknowledgments, and other required certifications **mandatory before access is granted.**

Page 17

- **Specific timeframe added:** Changes “promptly” to a defined requirement to review and adjust access rights **within five (5) business days of notification** of a personnel status change.
- **Immediate action added:** Requires access to be reviewed and adjusted **immediately** when there is:
 - Separation
 - Loss of authorization
 - Elevated security risk
- **Requirement strengthened:** Changes “may recover” to “**shall recover,**” making the recovery of Coalition-owned equipment, credentials, badges, authentication devices, records, and other organizational assets **mandatory** upon or prior to separation.

Page 18

- **Review frequency established:** Changes “periodically reviewed” to a specific requirement of **at least quarterly review.**
- **Scope clarified:** The quarterly review requirement applies specifically to systems containing **confidential, restricted, financial, personnel, or programmatic data.**

Page 21

- **Review frequency established:** Changes “reviewed periodically” to “**reviewed at least quarterly.**”
- **Scope clarified:** The quarterly review requirement specifically applies to systems containing **confidential, restricted, financial, personnel, or programmatic data.**
- **Requirement strengthened:** Changes “are recovered where applicable” to “**shall be recovered,**” making asset recovery mandatory.
- **Timing established:** Adds a specific requirement that physical and digital assets be recovered **prior to or upon separation.**
- **Exception process added:** Allows an exception only when **documented and approved by the CAO or Designee.**
- **Requirement strengthened:** Changes “may implement” to “**shall implement,**” making the implementation of the listed security controls **mandatory rather than discretionary.**

Page 22

- **Review frequency established:** Changes “reviewed and maintained periodically” to “reviewed and maintained at least annually.”
- **Additional review trigger added:** Requires review following **material network, firewall, or security architecture changes.**
- **Requirement strengthened:** Changes “may implement” to “shall implement,” making these security controls mandatory rather than discretionary.
- **Specific controls identified:** The updated language explicitly requires **intrusion detection, intrusion prevention, threat monitoring, alerting, and security event logging.**
- **Risk-based implementation added:** Requires the controls to be implemented **commensurate with system risk and operational requirements.**

Page 23

- **Requirement strengthened:** Changes “be evaluated when appropriate” to a requirement that changes **be evaluated before implementation**, making the review mandatory rather than discretionary.
- **Evaluation criteria added:** Requires consideration of **security, operational, privacy, and compliance impacts.**
- **Timing clarified:** Specifies that the evaluation must occur **before implementation.**
- **Emergency exception added:** Allows the evaluation requirement to be handled under **emergency change procedures** when applicable.
- **Specific timeframe added:** Changes “in a timely manner” to a defined requirement to apply critical security patches **within fifteen (15) calendar days of release.**
- **Expedited patching added:** Requires patches to be applied **sooner** when:
 - Active exploitation exists
 - Vendor guidance recommends immediate action
 - A risk assessment indicates immediate action is necessary

Page 24

- **“Where appropriate” removed** — documentation is now required rather than discretionary.
- **Documentation requirements expanded** to include:
 - Date the update/patch was applied
 - Affected systems
 - Exceptions
 - Failed updates
 - Remediation status



**Early Learning
Coalition** OF Marion
County

9/10/2026

Information Technology Policy Manual

LaTrisha Sims, Chief Executive Officer

Board approved June 25, 2026

Effective July 1, 2026

Revision R1 Effective: September 10, 2026

Board Approved: TBD



IT100 – IT Governance and Administration.....	4
IT100.01 Purpose and Scope	4
Inserted: 60GG-2 Alignment and Gap Closure	4
IT100.02 IT Governance and Oversight	5
IT100.03 Roles and Responsibilities	6
IT100.04 Ethics and Responsible Use	6
IT100.05 Legal and Regulatory Compliance.....	7
IT100.06 Policy Review and Governance	8
IT100.07 Electronic Records and Electronic Signatures *Added*	8
IT110 – Information Security	9
IT110.01 Security Governance.....	9
Inserted: Cybersecurity Risk Assessment and Risk Management.....	9
IT110.02 Data Classification and Protection.....	9
IT110.03 Identity & Access Management (IAM).....	10
IT110.04 Security Operations (endpoint, patching, monitoring).....	14
Inserted: Security Continuous Monitoring and Detection Requirements	14
IT110.05 Incident Response & Reporting	14
Inserted: Incident Classification, Reporting, and Lessons Learned	15
IT110.06 Remote Access and Virtual Private Network (VPN).....	15
IT110.07 Security Awareness and Training	16
IT110.08 Personnel Security.....	17
IT120 – User Access Management.....	19
IT120.01 User Account Management.....	19
IT120.02 Access Authorization and Approval	20
IT120.03 Password Standards	21
IT120.04 Multi-Factor Authentication.....	21
IT120.05 Access Review and Termination.....	22
IT130 – Network and System Security	23
IT130.01 Network Security Controls.....	23
IT130.02 Firewall and Intrusion Protection.....	24



IT130.03 System Configuration and Hardening	24
IT130.04 Software Updates and Patch Management.....	25
IT130.05 Endpoint Security	26
IT130.06 Bring Your Own Device (BYOD) Policy	26
IT130.07 Mobile Device Security	27
IT130.08 Physical Security and Environmental Controls	28
IT140 – Data Management and Protection	30
IT140.01 Data Classification & Retention.....	30
IT140.02 Data Storage Standards	31
IT140.03 Backup and Restoration	32
IT140.04 Data Recovery.....	32
IT140.05 Records Retention, Legal Hold, and Disposal.....	33
IT150 – Acceptable Use and Communication Systems	33
IT150.01 The Coalitional Email & Communication Use.....	33
IT150.02 Monitoring Notice.....	34
IT150.03 Phishing and Cybersecurity Awareness	35
IT150.04 User Responsibility & Training.....	36
IT150.05 Generative Artificial Intelligence (GenAI) Use.....	37
IT150.06 Social Media and Online Communications	38
IT160 – Technology Assets and Lifecycle.....	40
IT160.01 IT Asset Inventory	40
IT160.02 Equipment Issuance and Tracking	41
IT160.03 Maintenance and Support	42
IT160.04 Disposal of IT Equipment	42
IT170 – Vendor and Third-Party Management.....	43
IT170.01 – Vendor and Third-Party Management.....	43
IT170.02 Technology Vendor Selection	44
IT170.03 Third-Party Security Requirements.....	44
IT170.04 Vendor System Access	45
IT180 – Policy Compliance and Enforcement.....	46



IT180.01 Monitoring and Enforcement.....	46
IT180.02 Violations.....	47
IT180.03 Policy Acknowledgment.....	47
IT180.04 Exceptions and Risk Acceptance	48
Appendix A – Definitions.....	49
Appendix B – References and IT Policy Mapping Matrix	54
PART I – REFERENCES	54
PART II – IT POLICY MAPPING MATRIX (IT100–IT180)	55



IT100 – IT Governance and Administration

IT100.01 Purpose and Scope

Reference Procedure:

The Early Learning Coalition of Marion County, Inc. Information Technology (IT) Policy Manual defines the governance, security, acceptable use, and management standards for all Coalition technology resources, systems, data, and electronic communications.

These policies apply to all individuals who access, use, manage, support, or store Coalition information or technology resources. This includes, but is not limited to employees (full-time, part-time, temporary), interns, volunteers, Board members, contractors, consultants, vendors, and any third party acting on behalf of the Coalition.

Covered Technology Resources

This policy applies to all The Coalition-owned, leased, managed, or approved systems and technologies, including:

- Computer hardware, laptops, desktops, and peripheral devices
- Networks, internet services, and telecommunications systems
- Cloud-based platforms, applications, and services
- Email, messaging, and collaboration tools.
- Mobile devices and remote access technologies
- Software, databases, and information systems
- Electronic records and digital data repositories
- Cybersecurity tools, monitoring systems, and security controls

Purpose

This manual exists to:

- Protect the confidentiality, integrity, and availability of The Coalition systems and data (CIA triad aligned with NIST principles)
- Ensure secure, ethical, and appropriate use of technology resources.
- Maintain compliance with applicable federal and State of Florida laws, Florida Department of Education and Division of Early Learning requirements, grant agreements, and contractual obligations.
- Establish consistent standards for governance, cybersecurity, data protection, and acceptable use.
- Reduce operational, legal, financial, and reputational risk to the Coalition.

This manual serves as the governing standard for all IT-related policies, procedures, and technical controls.

Inserted: 60GG-2 Alignment and Gap Closure

Alignment Intent. This policy manual is intended to align the Coalition's information technology and cybersecurity governance practices with the State of Florida Cybersecurity Standards in Chapter 60GG-2, Florida Administrative Code, including the five cybersecurity functions: Identify, Protect, Detect, Respond, and Recover.

Gap Closure Approach. To strengthen 60GG-2 alignment, the Coalition shall maintain documented controls, procedures, evidence, and review practices addressing asset management, governance, risk assessment, identity and access management, awareness and training, data security, continuous monitoring, incident response, recovery planning, and third-party risk management.

- **Identify:** Maintain asset inventories, assign system and data ownership, document cybersecurity risks, and track risk treatment or acceptance decisions.
- **Protect:** Enforce least privilege, MFA, security awareness training, secure configuration, patching, encryption, and data handling requirements.
- **Detect:** Maintain logging, monitoring, alert review, and escalation procedures for suspicious or unauthorized activity.
- **Respond:** Maintain incident classification, escalation, communication, containment, evidence preservation, and post-incident review procedures.
- **Recover:** Maintain backup, restoration, business continuity, disaster recovery, and recovery communication procedures.

IT100.02 IT Governance and Oversight

Reference Procedure:

This manual establishes the Coalition's governance structure for oversight, management, and accountability of information technology and cybersecurity practices.

The IT Policy Manual supersedes all prior IT-related policies, procedures, and informal directives, unless explicitly retained by the Coalition in writing.

Governance Authority

The Board of Directors and Executive Leadership are responsible for:

- Oversight of IT governance and cybersecurity risk management
- Ensuring alignment of technology operations with the Coalition's mission and strategic goals
- Supporting compliance with legal, regulatory, and contractual obligations
- Ensuring adequate resources and controls are in place to manage technology risk.

Standards and Controls

Executive Leadership ~~may~~ shall authorize:

- IT standards
- Technical procedures
- Security controls and configurations

All standards must:

- Align with this policy manual.



- Comply with applicable laws, regulations, and grant requirements.
- Support recognized cybersecurity frameworks (including NIST-aligned practices where applicable)

IT100.03 Roles and Responsibilities

Reference Procedure:

The Chief Administrative Officer (CAO), or designee, is responsible for oversight and administration of the Coalition's IT policies and compliance program.

CAO / IT Governance Responsibility

The CAO or designee ensures that:

- IT policies are implemented and enforced consistently.
- Required agreements (acceptable use, confidentiality, security awareness) are executed prior to system access.
- Compliance with cybersecurity, privacy, and grant requirements is maintained.

IT / Data Security Administration

The CAO or Designee and/or Data Security Administrator is responsible for operational access and system security, including:

- Creating and managing user accounts
- Assigning access based on least privilege and job function.
- Updating access based on role changes.
- Disabling access upon termination or separation
- Monitoring account activity and access controls
- Supporting cybersecurity monitoring and compliance activities

HR and Management Responsibilities

Human Resources and supervisory personnel must:

- Promptly notify IT of hiring, role changes, and separations
- Support enforcement of onboarding and offboarding controls.

User Responsibilities

All authorized users must:

- Follow all IT policies and security requirements.
- Protect credentials and authentication information.
- Safeguard The Coalition data and systems.
- Immediately report suspected security incidents, misuse, or policy violations.

IT100.04 Ethics and Responsible Use

Reference Procedure:

The Coalition technology resources are provided to support official business operations and mission delivery. These resources must be used in a professional, lawful, and responsible manner.

Acceptable Use Expectations

Users must:

- Use systems ethically, securely, and in accordance with applicable laws and policies.



- Exercise professional judgment in all technology-related activities.
- Protect Coalition data and technology assets from misuse or harm.

Limited personal use may be permitted only when:

- Explicitly authorized by Executive Leadership
- It does not interfere with job duties or operations.
- It does not introduce risk to systems, data, or compliance obligations.

Prohibited Activities

Users may not:

- Access or distribute unlawful, inappropriate, or offensive content.
- Conduct unauthorized business, political activity, or fundraising.
- Install or use unauthorized software, devices, or cloud services.
- Bypass security controls or monitoring systems.
- Share credentials or authentication tokens.
- Access systems or data without authorization
- Introducing malware or malicious code
- Alter or interfere with system security or operations.
- Misrepresent identity or misuse of Coalition systems or data.

Data Ownership and Privacy

All data created, stored, transmitted, or processed on The Coalition systems is the property of the Coalition, subject to applicable law.

Users should not expect personal privacy when using Coalition systems or devices.

The Coalition may shall monitor, access, and audit systems and activity at any time, consistent with law, security requirements, and operational needs.

Enforcement

Violations may result in disciplinary action up to and including termination, revocation of access, and potential legal consequences.

IT100.05 Legal and Regulatory Compliance

Reference Procedure:

The Coalition complies with all applicable federal, state, and local laws, regulations, executive orders, and contractual/grant requirements governing information technology and data use.

Compliance Areas Include:

- Data privacy and confidentiality requirements
- Protection of personally identifiable information (PII)
- Cybersecurity and information security standards
- Public records and retention requirements (as applicable)
- Software licensing and intellectual property laws
- Fraud prevention and safeguarding public funds.
- Employment and payroll system access requirements
- Federal and State of Florida grant compliance obligations



Compliance Expectations

Users must:

- Manage all The Coalition data in accordance with legal and contractual requirements.
- Avoid unauthorized disclosure or misuse of protected information.
- Follow the most restrictive requirement when policy and regulation differ (unless prohibited by law)

Failure to comply may result in disciplinary action, loss of access, termination, and legal consequences.

IT100.06 Policy Review and Governance

Reference Procedure:

Management, IT, and other designated stakeholders shall review this policy at least annually and following material changes to operations, technology, applicable laws, grant obligations, contractual requirements, or cybersecurity standards.

Revisions shall be made as needed to reflect changes in technology, law, regulation, funding requirements, or business operations. The Coalition shall issue supporting standards, procedures, and guidance documents as necessary to implement this policy.

Management, IT, and other designated stakeholders ~~will periodically~~ review this policy ~~to ensure it remains current with operational needs, legal requirements, grant obligations, and cybersecurity practices.~~

Revisions ~~may~~ be made to reflect changes in technology, law, regulation, funding requirements, or business operations. The Coalition ~~may~~ issue supporting standards, procedures, and guidance documents to implement this policy.

In the event of a conflict between this policy and a more restrictive law, regulation, grant requirement, or contractual obligation, the more restrictive requirement will control unless prohibited by law.

IT100.07 Electronic Records and Electronic Signatures *Added*

The Coalition may use electronic records and electronic signatures to conduct, document, approve, and retain business transactions when permitted by applicable law, regulation, funding requirements, contractual requirements, and ELCMC policy.

The Coalition shall maintain appropriate controls to ensure the integrity, security, confidentiality, authenticity, and auditability of electronic records and electronic signatures.

Electronic signatures shall:

- Be unique to the individual signer;

- Remain under the control of the individual signer;
- Be capable of verification;
- Be linked to the applicable electronic record or data in a manner that ensures that a material alteration or change to the signed data is detectable and, where supported by the electronic signature system, invalidates the signature; and
- Be associated with the applicable electronic record in a manner that provides reasonable assurance of the signature's authenticity and the integrity of the signed record.

Electronic records shall be maintained in a manner that preserves their reliability, accessibility, integrity, and auditability for the applicable retention period.

IT110 – Information Security

IT110.01 Security Governance

Reference Procedure:

Coalition maintains an information security governance program to protect the confidentiality, integrity, and availability of all systems and data.

This program ensures:

- Clear accountability for cybersecurity risk management
- Alignment with operational needs and compliance obligations
- Consistency with recognized frameworks such as NIST cybersecurity principles

Security is a shared responsibility across Executive Leadership, IT administration, and all users.

Coalition reserves the right to implement technical, administrative, and physical safeguards necessary to protect Coalition assets and reduce cybersecurity risk.

Inserted: Cybersecurity Risk Assessment and Risk Management

The Coalition shall conduct periodic and event-driven cybersecurity risk assessments for information systems, technology services, cloud platforms, vendors, and material technology changes. Risk assessments shall consider threats, vulnerabilities, likelihood, impact, data sensitivity, business criticality, legal or grant obligations, and existing controls.

Identified risks shall be documented, assigned an owner, prioritized, and tracked through mitigation, transfer, avoidance, or documented acceptance. Risk acceptance shall require appropriate management approval, compensating controls where feasible, an expiration or review date, and supporting documentation retained for audit purposes.

IT110.02 Data Classification and Protection

Reference Procedure:

Coalition uses a data classification model to ensure appropriate handling of information based on sensitivity and regulatory requirements.



- Data Classification Levels
- Public – Approved for public release with no harm from disclosure.
- Internal Use Only – Non-public operational information
- Confidential – Sensitive information that may cause harm if disclosed.
- Restricted / Highly Sensitive – Information requiring highest protection (e.g., PII, HR records, financial data, grant-protected data)

Protection Requirements

All data must be:

- Accessed only by authorized individuals (least privilege)
- Stored only in approved The Coalition systems.
- Transmitted using secure, approved methods.
- Protected from unauthorized disclosure or modification.
- Prohibited from storage on personal or unmanaged systems.

IT110.03 Identity & Access Management (IAM)

Reference Procedure:

The Coalition enforces Identity and Access Management (IAM) controls to ensure secure, appropriate, and auditable access to all systems and data.

Access Standards

- Access shall be based on job roles, department needs, and the principle of least privilege.
- User accounts shall be unique to each individual and shall not be shared.
- Access must be approved prior to provisioning.
- Access shall be updated within five (5) business days of notification of job role, responsibility, or employment status changes, and sooner when elevated risk or separation requires immediate action.
- Access shall be removed immediately upon separation of employment or contract termination.
- Temporary accounts shall be time-limited and expire as required.

Authentication Requirements

- Users must authenticate using approved Coalition credentials.
- Multi-Factor Authentication (MFA) shall be required for remote access, privileged accounts, and systems containing confidential, restricted, financial, personnel, or programmatic data. Any technical limitation shall be documented through the exception and risk acceptance process.
- Credentials shall remain confidential and shall not be shared under any circumstances.

User Access Reviews

To ensure access rights remain appropriate and consistent with job responsibilities, the Coalition shall perform user access reviews at least quarterly for systems containing



confidential, restricted, financial, personnel, or programmatic data and within five (5) business days of notice of a material personnel status change.

Quarterly Access Reviews

User access for systems containing confidential, restricted, financial, personnel, or programmatic data shall be reviewed at least quarterly to ensure:

- Access remains appropriate for the user's current role.
- Excessive or unnecessary privileges are not present.
- Administrative access remains justified.
- Terminated or inactive accounts have been removed or disabled.
- Temporary accounts have not exceeded approved time limits.

Personnel Change Reviews

Access rights shall be reviewed and adjusted immediately upon:

- New hire onboarding
- Employee transfer or promotion
- Change in job responsibilities.
- Extended leave of absence
- Contractor or vendor engagement completion
- Employee or contractor separation

Access Provisioning and Deprovisioning

The Coalition shall maintain documented procedures for the full lifecycle of user access, including:

- User account creation
- Access approval and authorization
- Privileged account assignment
- Modification of access rights
- Account suspension
- Account termination

All system access for separated employees, contractors, interns, volunteers, and vendors shall be disabled no later than the individual's final working day or immediately upon notification of involuntary separation, elevated security risk, or revoked authorization, unless an alternate timeframe is formally approved, documented, and supported by compensating controls.

Administration and Oversight

Information Technology is responsible for provisioning, modifying, and removing system access in accordance with approved procedures, segregation of duties, and least privilege principles. System owners, supervisors, the Chief Administrative Officer, or authorized CAO or Designees shall ensure access remains appropriate and aligned with job responsibilities.

Audit Logging

Systems containing confidential, financial, personnel, or programmatic information shall maintain audit logs sufficient to record the following events. Any system unable to support required logging shall be documented through the exception and risk acceptance process.

- User login and logout activity
- Access to sensitive or confidential data
- Privileged account activity
- Changes to security settings
- Changes to access permissions
- Changes affecting financial transactions, assets, or program data.

Audit logs shall be retained and reviewed in accordance with applicable security requirements, compliance obligations, and the Coalition's records retention schedule.

60GG-2 Function	Category	Policy Area	Control Intent	Evidence / Documentation	Owner	Review Frequency
Identify	Asset Management / Governance / Risk Assessment	IT100 , IT110 , IT160 , IT170	Maintain system ownership, inventories, governance oversight, vendor visibility, and documented cybersecurity risks.	Asset inventory, risk register, vendor review records, governance approvals.	Executive Leadership / CAO or Designee	At least annually and upon major change
Protect	Access Control / Awareness / Data Security / Protective Technology	IT110 , IT120 , IT130 , IT140 , IT150	Protect systems and data through least privilege, MFA, secure configuration, patching, endpoint protection, encryption, training, and	Access approvals, MFA records, training logs, patch reports, configuration standards.	CAO or Designee / System Owners	Quarterly or as control requires



			acceptable use controls.			
Detect	Anomalies and Events / Continuous Monitoring / Detection Processes	IT110 , IT130 , IT180	Detect suspicious activity through logging, monitoring, alert triage, and escalation.	Security logs, alert tickets, monitoring reports, escalation records.	CAO or Designee / IT Support	Ongoing with periodic review
Respond	Response Planning / Communications / Analysis / Mitigation / Improvements	IT110 , IT150 , IT180	Respond to incidents through reporting, classification, containment, evidence preservation, communication, mitigation, and corrective action.	Incident reports, root-cause analysis, notification decisions, lessons-learned records.	Executive Leadership / CAO or Designee	After each incident and at least annually
Recover	Recovery Planning / Improvements / Communications	IT140 , IT180	Restore systems and operations through backup, restoration testing, recovery procedures, communications, and plan updates.	Backup logs, restoration test results, recovery plans, after-action updates.	CAO or Designee / System Owners	At least annually and after significant incidents



IT110.04 Security Operations (endpoint, patching, monitoring)

Reference Procedure:

The Coalition maintains security operations to protect systems from threats and vulnerabilities.

Endpoint Security

- All The Coalition devices must follow approved security configurations.
- Security tools (e.g., antivirus/EDR) must remain active.
- Users may not disable or bypass security controls.

Patch Management

- Systems must remain current with security updates.
- Critical updates shall be required immediately when necessary to address significant security risk.
- Users may not delay or interfere with required updates.

Monitoring and Logging

- Systems shall be monitored for security, compliance, and operational purposes.
- Activity shall be logged, reviewed, and audited.
- Users have no expectation of privacy on The Coalition systems.

Inserted: Security Continuous Monitoring and Detection Requirements

Security-relevant events shall be logged and reviewed based on documented system classification, data sensitivity, and risk assessment results. Monitoring shall include privileged account activity, failed login attempts, malware or endpoint alerts, firewall or intrusion alerts, unauthorized configuration changes, unusual data access, and other indicators of compromise unless an exception is formally approved, documented, and reviewed at least annually.

Alerts and anomalies shall be triaged, escalated, documented, and retained in accordance with applicable retention, contractual, grant, and cybersecurity requirements. Logging or monitoring exceptions shall be documented through the exception and risk acceptance process.

IT110.05 Incident Response & Reporting

Reference Procedure:

The Coalition maintains an incident response program to ensure timely identification, containment, investigation, recovery, and documentation of security incidents.

Security incidents include, but are not limited to, data breaches or suspected breaches, unauthorized system or data access, malware, ransomware, phishing, lost or stolen devices, accidental disclosure of sensitive information, and any event that may affect the confidentiality, integrity, or availability of The Coalition systems or data.

The Coalition's incident response process will include the following phases:



- Preparation.
- Detection and analysis.
- Containment, eradication, and recovery.
- **Post**-incident review and corrective action.

All users must immediately report suspected incidents to their supervisor and/or CAO or Designee, and no later than twenty-four (24) hours after discovery. IT shall assess the event, assign a severity level, document the determination, and coordinate required response actions, including account isolation, credential resets, system containment, legal or management notification, and external reporting when required.

For all confirmed security incidents and suspected incidents involving confidential, restricted, financial, personnel, or programmatic data, the Coalition shall document the incident, preserve relevant evidence, conduct root-cause analysis, and implement corrective actions to reduce the likelihood of recurrence. Failure to report a suspected incident may result in disciplinary action and potential legal or regulatory consequences.

Inserted: Incident Classification, Reporting, and Lessons Learned

Security incidents shall be classified based on severity, scope, affected systems, data sensitivity, operational impact, legal or grant implications, and potential harm. The Coalition shall maintain internal reporting and escalation procedures that define notification expectations for executive leadership, legal counsel, system owners, affected stakeholders, grantors, regulators, law enforcement, or external partners when required.

For incidents classified as moderate, high, or critical under the Coalition's incident severity procedures, the Coalition shall document response actions, preserve relevant evidence, evaluate notification obligations, perform root-cause analysis, identify corrective actions, and conduct a post-incident lessons-learned review within thirty (30) calendar days of incident closure. Lessons learned shall be used to update policies, procedures, technical controls, training, and recovery plans as appropriate.

IT110.06 Remote Access and Virtual Private Network (VPN)

Reference Procedure:

Remote access is provided only to support authorized business functions while maintaining the confidentiality, integrity, and security of The Coalition systems and data.

Authorization

- Remote access must be explicitly approved by IT or designated authority.
- Access is granted only to users with a legitimate business need.
- Access is role-based and subject to least privilege.

Secure Connection Requirements

- Approved VPN or secure remote access solutions must be used.
- All remote connections must use encryption approved by IT standards.

- Split tunneling shall be prohibited unless explicitly approved by the CAO or Designee, supported by a documented business need, and reviewed through the exception and risk acceptance process.
- Unapproved remote access methods are prohibited.

Device Requirements

- Only Coalition-approved or managed devices shall access internal systems remotely unless a documented BYOD exception is approved by the CAO or Designee and supported by required security controls.
- Devices must meet minimum security standards (endpoint protection, patching, encryption)
- Jailbroken, rooted, or unmanaged devices are prohibited.

Authentication & MFA

- Remote access requires Multi-Factor Authentication (MFA)
- Credentials must not be shared under any circumstances.

Monitoring & Security Controls

- Remote access sessions shall be logged, monitored, and audited.
- Suspicious or unauthorized remote access activity shall be reviewed by IT or the CAO or Designee, documented, and may result in immediate suspension or termination of access when necessary to protect Coalition systems or data.
- Users have no expectation of privacy when using remote access systems.

Prohibited Use

- Bypassing VPN or security controls
- Using public/shared unsecured networks without approved safeguards
- Establishing unauthorized remote connections into The Coalition systems

IT110.07 Security Awareness and Training

Reference Procedure:

Security Awareness Training

The Coalition shall maintain a formal Security Awareness and Training Program designed to promote the protection of confidential information, information systems, and technology resources.

All employees, temporary staff, contractors, interns, volunteers, and other authorized users with access to The Coalition information systems or confidential information shall complete required security awareness training.

The Security Awareness and Training Program shall include:

New Hire Training

- Security awareness training shall be completed within thirty (30) days of hire or before access to confidential information systems is granted, whichever occurs first.

Annual Refresher Training

- All users shall complete annual security awareness training at least once every twelve (12) months.

Required Training Topics

Training shall address, at a minimum:

- Protection of confidential, restricted, and personally identifiable information (PII).
- Data privacy and confidentiality requirements.
- Password security and authentication practices.
- Multi-Factor Authentication (MFA).
- Social engineering attacks.
- Phishing, smishing, and vishing threats.
- Malware and ransomware awareness.
- Secure email practices.
- Remote work and mobile device security.
- Physical security and workstation protection.
- Incident reporting procedures.
- Artificial Intelligence (AI) and Generative AI security risks.
- Acceptable Use requirements.

Ongoing Awareness Activities

The Coalition shall conduct at least one ongoing cybersecurity awareness activity each quarter, which may include phishing simulations, security bulletins, cybersecurity alerts, micro-training modules, refresher reminders, or awareness campaigns.

- Phishing simulations.
- Security bulletins and newsletters.
- Cybersecurity alerts.
- Micro-training modules.
- Refresher reminders and awareness campaigns.

Training Documentation

Records of completed training, acknowledgments, certifications, and awareness activities shall be maintained in accordance with applicable records retention requirements.

IT110.08 Personnel Security**Reference Procedure:**

The Coalition maintains personnel security controls to help protect confidential information, technology resources, and organizational assets from unauthorized access, misuse, disclosure, or compromise.

Personnel security controls support compliance with applicable laws, Division of Early Learning requirements, grant obligations, and organizational risk management practices.

Personnel Screening



The Coalition shall conduct pre-employment screening, background checks, reference verification, credential verification, and other personnel review activities when required by applicable laws, regulations, funding requirements, position responsibilities, or organizational policy.

Screening requirements shall be determined and documented based on:

- Position responsibilities
- Access to confidential, restricted, or sensitive information
- Access to financial systems or records
- Access to technology systems or administrative privileges
- Contractual, grant, licensing, or regulatory requirements

Employment, volunteer service, contractor engagement, or system access may be conditioned upon successful completion of required screening activities.

Confidentiality and Acknowledgments

Individuals granted access to Coalition information, systems, or technology resources shall be required to execute confidentiality agreements, acceptable use acknowledgments, security awareness acknowledgments, or other required certifications before access is granted.

Such acknowledgments may confirm that individuals:

- Understand their responsibilities for protecting Coalition information and systems.
- Agree to comply with applicable policies, procedures, and security requirements.
- Understand monitoring, auditing, and compliance expectations.
- Acknowledge potential disciplinary, contractual, or legal consequences for noncompliance.

Access Authorization

Access to Coalition systems, applications, networks, facilities, and information shall be granted only when:

- A legitimate business need exists.
- Appropriate authorization has been obtained.
- Required onboarding and security requirements have been completed.
- Access is consistent with assigned job duties and responsibilities.

Access shall be assigned in accordance with the principles of least privilege and need-to-know.

Personnel Change Reviews

Access rights shall be reviewed and adjusted within five (5) business days of notification of personnel status changes and immediately when separation, loss of authorization, or elevated security risk occurs, including:

- New hire onboarding
- Transfers or promotions
- Changes in job responsibilities



- Extended leaves of absence
- Contractor or vendor engagement completion
- Separation of employment or service

The Coalition shall ensure that access privileges remain appropriate throughout the individual's relationship with the organization.

Separation and Access Removal

Upon termination of employment, contract completion, volunteer separation, or loss of authorization, access to Coalition systems, applications, facilities, and information shall be removed or disabled in accordance with established access management procedures.

The Coalition shall recover Coalition-owned equipment, credentials, identification badges, authentication devices, records, and other organizational assets prior to or upon separation.

Personnel Security Responsibilities

All personnel with access to Coalition information or technology resources are responsible for:

- Protecting confidential, restricted, and sensitive information
- Complying with applicable IT, cybersecurity, privacy, and confidentiality requirements
- Reporting suspected security incidents, policy violations, or unauthorized access
- Maintaining appropriate safeguards over assigned systems, credentials, and organizational assets

Failure to comply with personnel security requirements may result in disciplinary action, restrictions or revocation of access privileges, contract termination, legal action, or other corrective measures consistent with Coalition policy and applicable law.

IT120 – User Access Management

IT120.01 User Account Management

Reference Procedure:

Coalition implements formal user account management controls to ensure that access to information systems is secure, appropriate, and aligned with job responsibilities.

User accounts provide access to Coalition systems and data and must be managed in a controlled and auditable manner throughout the entire user lifecycle, including onboarding, role changes, and separation.

Account Management Requirements

All user accounts must:



- Be uniquely assigned to an individual user (shared accounts are prohibited unless explicitly approved for system-level functions)
- Be created only after proper authorization and completion of required onboarding documentation.
- Be configured based on the principle of least privilege.
- Be linked to valid employment, contract, volunteer, or authorized business need.
- Be maintained in accordance with system security standards and audit requirements.

Account Lifecycle Controls

User accounts must be:

- Provisioned only upon verified authorization
- Modified promptly when job responsibilities change.
- Disabled immediately upon separation or loss of authorization.
- Reviewed at least quarterly for continued necessity and appropriateness for systems containing confidential, restricted, financial, personnel, or programmatic data.

The CAO or Designee or Designee is responsible for ensuring account management processes are consistently applied and properly documented.

IT120.02 Access Authorization and Approval

Reference Procedure:

Access to Coalition systems, applications, and data is granted only through formal authorization processes to ensure appropriate control and accountability.

Access must always be based on legitimate department needs and assigned job responsibilities.

Authorization Principles

The Coalition applies the following principles:

- Least Privilege – Users are granted only the minimum access necessary to perform assigned duties.
- Need-to-Know – Access to sensitive or restricted information is limited to authorized personnel with a defined business purpose.
- Role-Based Access Control (RBAC) – Access is assigned based on standardized job roles whenever possible.

Approval Requirements

All access requests must:

- Be requested by the appropriate supervisor or authorized manager.
- Be approved by CAO or designee for authorization principals.
- Be reviewed by IT or designated system administrators prior to provisioning.
- Be documented and retained for audit and compliance purposes.

Access may be denied or modified if:

- It exceeds job requirements.
- It presents a security or compliance risk.



- It conflicts with grant, contractual, or regulatory obligations.

Excessive or unnecessary access increases the risk of unauthorized disclosure, system misuse, and compliance violations and is prohibited.

IT120.03 Password Standards

Reference Procedure:

Passwords are a critical component of the Coalition's cybersecurity controls and must be created, managed, and protected in a secure manner.

Weak or improperly managed passwords significantly increase the risk of unauthorized access and compromise of The Coalition systems and data.

Password Requirements

All passwords must:

- Meeting minimum complexity standards defined by IT security procedures
- Be unique and not reused across systems or personal accounts.
- Not be shared with any other individual under any circumstances.
- Be changed if compromise is suspected or confirmed.

Prohibited Practices

Users may not:

- Write down passwords in unsecured or visible locations.
- Store passwords in unapproved files, documents, or applications.
- Share passwords via email, text message, or other unsecured channels.
- Use easily guessable passwords (e.g., names, birthdays, simple words)
- Reuse previously compromised passwords.

Secure Storage

Where password storage tools are permitted, they must be:

- Approved by the Coalition
- Encrypted and secured according to IT standards.
- Access-controlled and monitored.

Users are responsible for safeguarding credentials and immediately reporting suspected compromise.

IT120.04 Multi-Factor Authentication

Reference Procedure:

The Coalition implements Multi-Factor Authentication (MFA) to strengthen identity verification and reduce the risk of unauthorized access.

MFA requires users to provide two or more verification factors when accessing designated systems, applications, or data environments.

MFA Requirements

Where implemented, MFA is:

- Required for all remote access to The Coalition systems.



- Required for access to sensitive, confidential, or restricted systems and data.
- Required for administrative or privileged accounts.
- Enforced based on risk level and system classification.

Approved Authentication Factors May Include:

- Something you know (password or PIN)
- Something you have (mobile device, authentication token, security key)
- Something you are (biometric verification, where approved)

User Responsibilities

Users must:

- Complete MFA enrollment as required.
- Maintain access to registered authentication devices.
- Immediately report loss or compromise of authentication devices
- Not attempting to bypass or disable MFA controls.

MFA controls are a mandatory security requirement and may not be waived without documented executive and IT security approval.

IT120.05 Access Review and Termination

Reference Procedure:

Coalition conducts regular access reviews and enforces strict termination procedures to ensure that system access remains appropriate, current, and secure.

Access Reviews

Access to Coalition systems and data must be:

- **Reviewed at least quarterly by IT and system owners for systems containing confidential, restricted, financial, personnel, or programmatic data.**
- Verified against current job roles and responsibilities.
- Adjusted or removed when no longer required.

Access reviews support compliance with audit requirements, grant obligations, and cybersecurity best practices.

Access Termination

User access must be terminated immediately when:

- Employment or contract ends.
- Job responsibilities no longer require system access.
- Authorization is revoked for any reason.
- Security risk or policy violation is identified.

Termination Process

Upon separation or access removal:

- All system access is disabled without delay.
- Credentials are revoked or reset.
- Access to email, applications, and cloud systems is removed.

- Physical and digital assets shall be recovered prior to or upon separation, unless a documented exception is approved by the CAO or Designee.
- Access logs may be retained for audit and investigative purposes.

Failure to properly terminate access increases the risk of unauthorized system entry and is considered a serious security control failure.

IT130 – Network and System Security

IT130.01 Network Security Controls

Reference Procedure:

The Coalition maintains network security controls to protect information systems, data, and technology resources from unauthorized access, disruption, misuse, or cyber threats.

Network infrastructure must be managed in a secure manner consistent with operational requirements, cybersecurity best practices, and applicable legal and contractual obligations.

Security Control Requirements

The Coalition shall implement security controls including:

- Network segmentation and access restrictions.
- Secure wireless network configurations
- Traffic filtering and network monitoring
- Encrypted communications and secure transmission methods
- Access controls for internal and external network connections
- Security logging and monitoring technologies

Authorized Access

Access to The Coalition networks is limited to:

- Authorized users
- Approved devices and systems
- Legitimate business purposes

Unauthorized access to The Coalition networks, systems, or communications infrastructure is prohibited.

Wireless Networks

Wireless networks must:

- Use approved encryption and authentication methods.
- Be configured and managed by authorized CAO or Designee
- Restrict unauthorized or guest access as appropriate.

Users may not install or operate unauthorized wireless access points, routers, or network-connected devices on The Coalition systems or facilities.



IT130.02 Firewall and Intrusion Protection

Reference Procedure:

Coalition utilizes firewall protections and intrusion detection/prevention controls to safeguard systems and networks from unauthorized access and malicious activity.

Firewall Requirements

Firewalls must:

- Be implemented at appropriate network boundaries.
- Restrict unauthorized inbound and outbound traffic.
- Be configured according to approved security standards.
- Be reviewed and maintained at least annually and after material network, firewall, or security architecture changes.

Changes to firewall rules or security configurations must be authorized and documented.

Intrusion Detection and Prevention

The Coalition shall implement intrusion detection, prevention, threat monitoring, alerting, and security event logging controls commensurate with system risk and operational requirements.

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Threat monitoring and alerting tools
- Security event logging and analysis technologies

These controls help identify, prevent, and respond to suspicious or malicious activity.

Users may not bypass, disable, interfere with, or attempt to circumvent firewall or intrusion protection controls.

IT130.03 System Configuration and Hardening

Reference Procedure:

The Coalition establishes system configuration and hardening standards to reduce vulnerabilities and improve overall system security.

Secure Configuration Standards

Systems, devices, applications, and servers must:

- Be configured according to approved security baselines.
- Disable unnecessary services, ports, and accounts.
- Utilize secure authentication and access settings.
- Apply security configurations appropriate to system function and risk level.

Administrative Controls

Only authorized personnel may:

- Modify system configurations.
- Install system software or utilities.



- Change security settings or administrative controls.

Default passwords, factory settings, and unnecessary default accounts must be changed or disabled prior to deployment.

Change Management

Significant system configuration changes must:

- Be documented and approved where required.
- **Be evaluated for security, operational, privacy, and compliance impact before implementation unless emergency change procedures apply.**
- Minimize operational and security risk.

Improper or unauthorized system modifications are prohibited.

IT130.04 Software Updates and Patch Management

Reference Procedure:

The Coalition maintains patch management processes to ensure systems and applications remain protected against known vulnerabilities and security threats.

Update Requirements

Operating systems, applications, firmware, and security tools must:

- Be maintained with current vendor-supported security updates.
- **Receive critical security patches within fifteen (15) calendar days of release or sooner when active exploitation, vendor guidance, or risk assessment indicates immediate action is required.**
- Be monitored for known vulnerabilities and security advisories.

User Responsibilities

Users may not:

- Disable automatic updates or security tools.
- Delay required security updates without authorization.
- Install unapproved software updates or applications.

IT Responsibilities

Authorized CAO or Designee are responsible for:

- Managing patch deployment processes
- Evaluating critical vulnerabilities and risks
- Prioritizing remediation activities based on risk and operational impact.
- **Maintaining documentation of update and patching activities, including date applied, affected systems, exceptions, failed updates, and remediation status.**

Systems that cannot be updated or supported may be restricted, isolated, or removed from service.



IT130.05 Endpoint Security

Reference Procedure:

The Coalition maintains endpoint security controls to protect workstations, laptops, servers, mobile devices, and remote access systems from malware, unauthorized access, and cybersecurity threats.

Endpoint Protection Requirements

All The Coalition-owned or managed endpoints must:

- Utilize approved antivirus and/or endpoint detection and response (EDR) solutions.
- Maintain active and current malware protection.
- Be configured with approved security settings.
- Receive required security updates and patches.

Email systems, attachments, downloads, and internet-based content may be automatically scanned for malicious activity.

Remote Access Devices

Any device authorized for remote access to The Coalition systems must:

- Meet Coalition security standards.
- Maintain current antivirus and endpoint protection software.
- Utilize approved encryption and authentication controls where applicable.

User Restrictions

Users may not:

- Disable or bypass endpoint protection tools.
- Install unauthorized security software or utilities.
- Interfere with monitoring, logging, or security configurations.

The Coalition reserves the right to isolate, disable, or remove devices that present a security risk.

IT130.06 Bring Your Own Device (BYOD) Policy

Reference Procedure:

The use of personally owned devices to access Coalition systems or information is permitted only when authorized by Coalition and managed in accordance with security requirements.

Authorized BYOD Use

Approved personal devices may be used for limited business purposes only when:

- Access is authorized by executive leadership and/or CAO or Designee
- The device meets The Coalition security requirements.
- Appropriate security controls are implemented.

Security Requirements

Personally owned devices used for The Coalition business must:

- Maintain current operating system and security updates.
- Utilize password protection or biometric authentication.



- Use approved antivirus or endpoint protection where applicable.
- Support encryption and remote wipe capabilities if required.
- Connect only through approved secure access methods.

Data Protection

The Coalition data accessed or stored on personal devices remains the property of the Coalition and must be protected from unauthorized access, disclosure, or loss.

Users may not:

- Store restricted or extremely sensitive data on personal devices unless explicitly authorized.
- Share devices used for The Coalition business in a manner that compromises security.
- Circumvent mobile device management or security requirements.

Monitoring and Enforcement

The Coalition reserves the right to:

- Restrict or revoke BYOD access at any time.
- Require removal of Coalition data from personal devices.
- Enforcing security controls necessary to protect Coalition systems and information

Failure to comply with BYOD requirements may result in revocation of access, disciplinary action, or other corrective measures.

IT130.07 Mobile Device Security

Reference Procedure:

Coalition maintains security controls for mobile devices used to access, store, transmit, or process The Coalition information or systems.

Mobile devices, including laptops, tablets, smartphones, and portable computing devices, provide operational flexibility but also present increased cybersecurity and data protection risks.

Security Requirements

Mobile devices authorized for The Coalition business must:

- Utilize approved security configurations and access controls.
- Be protected through passwords, biometrics, encryption, or other approved authentication methods.
- Maintain current operating system and security updates.
- Utilize approved antivirus, endpoint protection, or mobile device management controls where applicable.
- Automatically locked after periods of inactivity where technically feasible

Protection of Coalition Information

Confidential, restricted, or sensitive Coalition information accessed through mobile devices must be protected against unauthorized access, disclosure, alteration, or loss.



Storage of confidential or restricted The Coalition data on unauthorized, unmanaged, or non-approved mobile devices is prohibited unless expressly authorized and protected through approved security controls.

Lost or Stolen Devices

Users must immediately report:

- Lost or stolen mobile devices.
- Suspected unauthorized access
- Compromised devices containing The Coalition information.

The Coalition may remotely disable, restrict, or remove access to protect The Coalitional systems and data.

User Responsibilities

Users are responsible for:

- Maintaining physical control of mobile devices
- Preventing unauthorized access or use
- Avoiding use of unsecured public networks without approved protection
- Complying with all applicable IT, cybersecurity, and acceptable use requirements

IT130.08 Physical Security and Environmental Controls

Reference Procedure:

Coalition maintains physical security and environmental controls to protect information systems, technology assets, facilities, and The Coalition information from unauthorized access, theft, damage, loss, or disruption.

Physical security safeguards are designed to support the confidentiality, integrity, and availability of The Coalition systems and information while reducing operational and cybersecurity risk.

Restricted Access Areas

Access to sensitive technology environments, including server rooms, network closets, telecommunications equipment areas, and other restricted technology spaces, must be limited to authorized personnel with a legitimate business need.

Physical access controls may include:

- Locked doors, key controls, badge access systems, or other approved access restrictions
- Visitor sign-in or access documentation procedures
- Monitoring or surveillance measures where appropriate
- Periodic review of authorized access permissions

Unauthorized individuals may not enter or remain in restricted technology areas without authorization.

Visitor Access and Escort Requirements

Visitors, vendors, contractors, and other non-authorized individuals accessing The Coalition facilities or restricted areas may be:



- Required to sign in or otherwise identify themselves.
- Escorted by authorized personnel while in restricted areas.
- Limited to approved business purposes and authorized locations only

Visitors must not be permitted unsupervised access to systems, confidential information, or restricted technology infrastructure unless specifically authorized.

Workstation and Device Security

Users are responsible for securing workstations, laptops, mobile devices, and other technology equipment from unauthorized access or viewing.

Security expectations include:

- Locking or logging off workstations when unattended
- Securing portable devices when not in use
- Preventing unauthorized viewing of confidential or restricted information
- Maintaining physical control of Coalition devices in office, remote, or public environments

Users may not leave sensitive information or unlocked devices unattended in unsecured locations.

Clean Desk and Information Protection

Users must take reasonable measures to protect confidential, restricted, or sensitive information in physical form.

Clean desk practices may include:

- Securing sensitive documents when unattended
- Removing confidential information from public view
- Safely storing records, removable media, and portable devices
- Avoiding unnecessary printing of sensitive information

Printed materials containing confidential or restricted information must be protected against unauthorized access or disclosure.

Environmental and Equipment Protection

Technology systems and equipment must be protected against environmental hazards and operational risks where appropriate.

Protective measures may include:

- Surge protection and power management controls.
- Climate or environmental controls for critical equipment
- Protection against water damage, fire, excessive heat, or other hazards
- Secure placement and storage of equipment to reduce theft or accidental damage risks.

The Coalition may restrict placement or use of technology equipment in locations that present unacceptable operational or security risks.

Secure Storage of Backup Media and Sensitive Materials



Backup media, removable storage devices, and other sensitive technology assets or records must be stored securely and protected from unauthorized access, damage, theft, or loss.

Where appropriate, storage protections may include:

- Locked cabinets, rooms, or secure storage containers
- Restricted access controls
- Offsite or environmentally protected storage locations
- Secure transport procedures for backup or recovery media

Disposal and Shredding Requirements

Paper records, removable media, and other materials containing confidential, restricted, or sensitive information must be disposed of using secure methods that prevent unauthorized access or reconstruction.

Approved disposal methods may include:

- Cross-cut shredding
- Locked disposal bins or shredding containers
- Secure destruction services
- Approved electronic media sanitization or destruction methods.

Users may not dispose of sensitive information in unsecured trash or recycling containers.

Failure to comply with physical security and environmental control requirements may result in disciplinary action, revocation of access privileges, and other corrective measures consistent with The Coalition policy.

IT140 – Data Management and Protection

IT140.01 Data Classification & Retention

Reference Procedure:

The Coalition maintains data classification and retention practices to ensure information is appropriately protected, managed, retained, and disposed of in accordance with operational needs, legal requirements, grant obligations, and applicable records management standards. (See Fiscal Policy for full Retention Policy)

Data Classification

The Coalition data must be classified based on sensitivity, confidentiality, regulatory requirements, and business impact.

Classification Levels

- **Public** – Information approved for public release.
- **Internal Use Only** – Non-public operational information intended for internal business purposes.



- **Confidential** – Sensitive information that could cause operational, financial, legal, or reputational harm if improperly disclosed.
- **Restricted / Highly Sensitive** – Information requiring the highest level of protection, including personally identifiable information (PII), employee records, financial information, and protected grant or contract data.

Retention Requirements

The Coalition records and data must be retained in accordance with:

- Applicable federal and State of Florida laws and regulations
- Florida public records and records retention requirements, where applicable
- Grant, contractual, and audit obligations
- Operational and business continuity needs

Data Disposal

When retention periods expire, data must be securely disposed of using approved methods that protect against unauthorized access or recovery.

Improper destruction, alteration, or unauthorized removal of The Coalition records or data is prohibited.

IT140.02 Data Storage Standards

Reference Procedure:

The Coalition maintains secure data storage practices to protect information from loss, corruption, unauthorized access, misuse, or unavailability.

Data storage controls are designed to support the confidentiality, integrity, and availability of The Coalition information and systems.

Approved Storage Requirements

The Coalition data must be stored only in:

- Approved The Coalition-managed systems.
- Authorized cloud platforms and applications
- Secure network locations or storage environments approved by IT.

Storage of The Coalition data on unauthorized systems, personal accounts, removable media, or unapproved cloud services is prohibited unless expressly authorized.

Protection Standards

Data storage solutions must include appropriate safeguards, which may include:

- Access controls based on least privilege
- Encryption where appropriate or required.
- Redundancy and availability protections
- Security monitoring and logging controls
- Backup and recovery capabilities

Data Availability

The Coalition must maintain appropriate backup copies and recovery capabilities for critical systems and data to support operational continuity and recovery from:



- Hardware or system failures
- Accidental deletion or modification
- Software corruption
- Cybersecurity incidents or malicious activity
- Natural disasters or other operational disruptions

Users are responsible for storing Coalition data in approved locations to ensure proper backup, retention, and protection.

IT140.03 Backup and Restoration

Reference Procedure:

The Coalition maintains backup and restoration processes to support business continuity, operational resilience, and recovery of critical systems and information.

Backup Requirements

Backup processes must:

- Protect critical systems, applications, and data.
- Be performed using approved methods and technologies.
- Be monitored periodically for successful completion.
- Be secured against unauthorized access, alteration, or deletion.
- Backup frequency and retention may vary based on:
 - Operational requirements
 - Data sensitivity
 - Regulatory or contractual obligations
 - System criticality and risk level

Restoration and Recovery

The Coalition must maintain the ability to restore critical systems and data within reasonable operational timeframes following a disruption or loss event.

Restoration capabilities may be periodically assessed or validated to ensure backup integrity and recovery effectiveness.

Security of Backups

Backup media and stored backup data must be:

- Protected from unauthorized access or disclosure.
- Stored securely, including offsite or cloud protections where appropriate.
- Managed in accordance with data classification requirements.

Unauthorized access to, alteration of, or deletion of backup data is prohibited.

IT140.04 Data Recovery

Reference Procedure:

Coalition maintains data recovery practices aligned with operational continuity, cybersecurity response, disaster recovery, and business resiliency objectives.



Data recovery planning supports the restoration of systems, services, and information following events that may disrupt normal operations.

Recovery Objectives

Recovery activities should prioritize:

- Protection of critical business functions
- Restoration of essential systems and data
- Reduction of operational downtime
- Preservation of data integrity and security
- Compliance with legal, grant, and reporting obligations

Coordination with Recovery and Continuity Efforts

Data recovery activities may be coordinated with:

- Incident response procedures
- Disaster recovery planning
- Business continuity operations
- Cybersecurity containment and remediation efforts

Testing and Validation

The Coalition may periodically review, assess, or validate recovery capabilities to:

- Confirm backup integrity.
- Evaluate recovery readiness.
- Identify gaps or operational risks.
- Improve resiliency and response effectiveness.

Recovery processes must be managed in a manner that minimizes disruption while maintaining the security and integrity of The Coalition systems and information.

IT140.05 Records Retention, Legal Hold, and Disposal

Reference Procedure:

The Coalition data and records must be retained, preserved, and disposed of in accordance with applicable federal and State of Florida requirements, grant conditions, public records obligations, and the Coalition's approved retention schedule.

When The Coalition data is subject to a legal hold, audit request, investigation, or litigation hold, normal disposal or deletion requirements are suspended until the hold is released by authorized management or legal counsel.

Users must not delete, alter, conceal, or dispose of The Coalition records outside approved retention and destruction procedures. Secure disposal must be performed using approved methods that prevent unauthorized recovery.

IT150 – Acceptable Use and Communication Systems

IT150.01 The Coalitional Email & Communication Use

Reference Procedure:



Coalition provides email, messaging, collaboration platforms, internet access, and other electronic communication systems to support official business operations and Coalition objectives.

All communication systems must be used in a professional, secure, lawful, and responsible manner consistent with The Coalition policies and applicable legal and regulatory requirements.

Authorized Use

The Coalition communication systems are intended primarily for authorized business purposes, including:

- Internal and external business communications
- Program operations and service delivery.
- Collaboration with authorized partners, vendors, and stakeholders
- Approved operational, administrative, and reporting functions.
- Limited personal use may be permitted when it:
 - Does not interfere with work responsibilities or operations.
 - Does not create security, legal, or operational risk.
 - Complies with all The Coalition policies and standards.

Prohibited Use

Users may not use The Coalition communication systems to:

- Transmit unlawful, offensive, discriminatory, harassing, or inappropriate content.
- Distribute malware, malicious links, or unauthorized attachments.
- Conduct unauthorized business, political activity, or fundraising.
- Misrepresent identity or impersonate another individual.
- Circumvent security controls or monitoring systems.
- Share confidential or restricted information without authorization.
- Subscribe to unauthorized services or applications using The Coalition accounts.

Email Security

Users must exercise caution when handling email communications, attachments, hyperlinks, and external messages.

Sensitive or restricted information may only be transmitted using approved secure methods and in accordance with data protection requirements.

Records and Retention

Electronic communications may constitute official business records and must be retained, preserved, or disclosed in accordance with applicable records retention requirements, legal obligations, and Coalition policies.

IT150.02 Monitoring Notice

Reference Procedure:

The Coalition technology systems, devices, networks, communication platforms, internet services, and electronic resources are the property of the Coalition and are subject to monitoring, review, and audit.



Monitoring Authority

To protect The Coalitional systems, data, and operations, Coalition reserves the right to:

- Monitor system and network activity.
- Review email, internet usage, and electronic communications.
- Access files, records, logs, and stored information
- Conduct security monitoring, auditing, and investigations.
- Preserve and disclose information when required for operational, legal, security, or compliance purposes.

Monitoring may occur with or without notice, consistent with applicable laws and operational requirements.

No Expectation of Privacy

Users should have no expectation of personal privacy when using:

- The Coalition-owned or managed systems
- The Coalitional email accounts
- Internet and network services
- Collaboration or communication platforms
- The Coalition-issued devices or storage systems

Personal use of The Coalition systems does not create any expectation of privacy or confidentiality.

Compliance and Investigations

Information obtained through monitoring may be used for:

- Cybersecurity and threat detection
- Compliance verification
- Operational support
- Investigations of suspected misconduct, policy violations, or unlawful activity

Unauthorized attempts to bypass monitoring or security controls are prohibited.

IT150.03 Phishing and Cybersecurity Awareness

Reference Procedure:

The Coalition maintains cybersecurity awareness practices to help protect systems, users, and data from phishing, social engineering, malware, ransomware, and other cybersecurity threats.

User Awareness Responsibilities

All users are responsible for:

- Remaining alert to suspicious communications or activity
- Exercising caution with unexpected emails, attachments, links, or requests for information
- Verifying the legitimacy of requests involving credentials, payments, sensitive information, or system access
- Following The Coalition cybersecurity guidance and reporting procedures



Phishing and Social Engineering

Users must not:

- Open suspicious attachments or links from unknown or unverified sources
- Provide passwords, MFA codes, or sensitive information in response to unsolicited requests.
- Circumvent security warnings or protections.

Suspected phishing attempts, scams, or malicious communications must be reported immediately to designated CAO or Designee or supervisors.

Security Awareness Activities

The Coalition may implement cybersecurity awareness activities including:

- Security awareness training
- Simulated phishing exercises
- Security bulletins and alerts
- User education and best practice guidance

Participation in required security awareness activities is mandatory for all applicable users.

IT150.04 User Responsibility & Training

Reference Procedure:

All authorized users share responsibility for protecting The Coalition technology resources, systems, and information.

Users are expected to understand and comply with all applicable IT, cybersecurity, privacy, and data protection requirements.

User Responsibilities

Users must:

- Use The Coalition systems in a secure and responsible manner.
- Protect passwords, credentials, and authentication devices.
- Safeguard confidential and restricted information.
- Report suspected of security incidents, policy violations, or unauthorized access immediately.
- Follow all applicable policies, standards, procedures, and security guidance.

Failure to comply with security requirements may result in disciplinary action, revocation of access, termination of employment or contract, and/or legal consequences.

Security Awareness and Training

The Coalition may require users to complete:

- IT security awareness training
- Acceptable use of acknowledgments
- Privacy and confidentiality training
- Phishing or cybersecurity education programs



- Additional role-based security training where appropriate

Training requirements may be mandatory upon hire, periodically thereafter, and whenever significant policy or security changes occur.

Acknowledgment of Responsibility

Users may be required to acknowledge in writing or electronically that they:

- Understand The Coalition IT policies and requirements.
- Agree to comply with security and acceptable use standards.
- Accept responsibility for safeguarding Coalition systems and information.

Failure to complete required training or acknowledgments may result in delayed, restricted, or revoked system access.

IT150.05 Generative Artificial Intelligence (GenAI) Use

Reference Procedure:

The Coalition may authorize the use of approved Generative Artificial Intelligence (GenAI) tools and services to support operational, administrative, research, communication, or business functions.

Use of GenAI technologies must be conducted in a secure, lawful, ethical, and responsible manner consistent with The Coalition policies, confidentiality obligations, cybersecurity requirements, and applicable intellectual property laws.

Authorized Use

Only The Coalition-approved GenAI platforms, applications, or services may be used for The Coalition business purposes unless otherwise authorized by Executive Leadership or designated CAO or Designee.

Users of approved GenAI systems must:

- Exercise professional judgment regarding the accuracy, appropriateness, and reliability of generated content.
- Independently review and validate AI-generated output prior to use, distribution, or reliance
- Ensure GenAI use complies with all applicable confidentiality, privacy, cybersecurity, records retention, acceptable use, and data protection requirements.
- Comply with all applicable copyright, trademark, licensing, and intellectual property laws and restrictions.

Prohibited Use

Users may not:

- Input confidential, restricted, sensitive, or non-public The Coalition information into unapproved or publicly accessible AI systems.
- Use GenAI tools in a manner that could disclose protected information, personally identifiable information (PII), financial data, employee information, client information, other confidential Coalition data.



- Use GenAI systems to generate unlawful, discriminatory, offensive, deceptive, plagiarized, or inappropriate content.
- Misrepresent AI-generated content as independently created work without appropriate review, attribution, or disclosure where required.
- Circumvent Coalition security, privacy, or acceptable use requirements through AI technologies.

Data Protection and Confidentiality

Users are advised that information submitted to publicly available or unapproved AI systems may:

- Become publicly accessible or externally retained.
- Be stored, processed, or reused by third-party providers.
- Be outside the Coalition's control or ability to permanently remove.

Accordingly, users must not disclose confidential, restricted, or sensitive Coalition information through unauthorized AI platforms or services.

Responsibility for Work Product

Users remain fully responsible for all content, communications, decisions, and work products created, modified, or distributed using GenAI tools.

Use of AI assistance does not eliminate the user's responsibility to:

- Verify accuracy and appropriateness of content.
- Preventing plagiarism or misrepresentation
- Ensure compliance with professional, legal, contractual, grant, and ethical obligations.
- Properly attribute or disclose external sources where appropriate.

Any violation of The Coalition policy, confidentiality obligations, intellectual property rights, or applicable law involving GenAI use may result in disciplinary action up to and including termination of employment or contract, revocation of access privileges, and potential legal consequences.

IT150.06 Social Media and Online Communications

Reference Procedure:

The Coalition recognizes that employees and authorized users may engage in personal use of social media, online forums, blogs, networking platforms, and other electronic communication channels.

Users are expected to conduct themselves in a professional, lawful, respectful, and responsible manner when engaging in online activities that may affect the Coalition, its employees, clients, partners, vendors, or operations.

This policy applies to the use of:

- Social media platforms
- Blogs, forums, and online communities



- Video sharing or streaming platforms
- Messaging or collaboration platforms
- Personal websites or online publications
- Any electronic communication platform where Coalition affiliation may be identified.

Confidentiality and Information Protection

Users may not post, disclose, transmit, or share confidential, restricted, proprietary, or non-public The Coalition information through social media or other online platforms.

Prohibited disclosures may include, but are not limited to:

- Personally identifiable information (PII)
- Client, family, employee, volunteer, or vendor information
- Financial or operational information
- Internal policies, procedures, reports, or communications
- Security-related information
- Grant, contract, or program information not approved for public release.

Users must comply with all confidentiality, privacy, cybersecurity, records retention, and acceptable use requirements when engaging in online communications.

Representation of the Coalition

Only authorized individuals may speak, post, publish, or communicate on behalf of the Coalition in an official capacity.

Users may not:

- Represent individual opinions as official The Coalition positions.
- Create unauthorized official The Coalition accounts or pages.
- Use The Coalition branding, logos, trademarks, or official imagery without authorization.
- Misrepresent their authority or affiliation with the Coalition.

When discussing matters that may relate to the Coalition, users should clearly distinguish individual opinions from official The Coalitional statements.

Professional Conduct

Users are expected to maintain professional and respectful conduct in online communications.

Users may not engage in:

- Harassment, discrimination, threats, or unlawful conduct
- Defamatory or knowingly false statements
- Disclosure of confidential or protected information
- Vulgar, obscene, or abusive conduct that violates The Coalition policies.
- Online activity that materially disrupts Coalition operations, violates law, or creates substantial Coalition risk.



Nothing in this policy is intended to restrict rights protected under applicable federal, state, or local law, including lawfully protected communications regarding wages, hours, or working conditions.

Use of Coalition Systems and Resources

Limited personal social media use during work hours may be permitted when:

- It does not interfere with work responsibilities.
- It does not consume excessive Coalition resources.
- It complies with all The Coalition IT, cybersecurity, confidentiality, and acceptable use requirements.

Users may not:

- Use Coalition email addresses to register personal online accounts without authorization.
- Use The Coalition systems to conduct unlawful, inappropriate, or unauthorized activity.
- Circumvent security controls or monitoring systems through social media or online platforms.

Photographs, Media, and Sensitive Information

Users may not post photographs, videos, recordings, or images of The Coalition facilities, employees, clients, families, volunteers, records, or operations without appropriate authorization and compliance with applicable privacy and confidentiality requirements.

Monitoring and Enforcement

Use of The Coalition-owned systems, devices, accounts, and networks remains subject to monitoring, logging, review, and audit in accordance with The Coalition policy.

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, revocation of system access, legal action, or other corrective measures consistent with applicable law and The Coalition policy.

IT160 – Technology Assets and Lifecycle

IT160.01 IT Asset Inventory

Reference Procedure:

The Coalition maintains an inventory of information technology assets to support operational management, cybersecurity, accountability, audit readiness, and compliance with applicable legal, regulatory, grant, and contractual requirements.

Technology assets include hardware, software, cloud services, mobile devices, network equipment, peripheral devices, and other systems used to store, process, or transmit Coalition information.

Inventory Requirements



The Coalition shall maintain inventory records for applicable technology assets, which may include:

- Asset type and description
- Unique inventory identifier, asset tag, or serial number
- Assigned user, department, or custodian.
- Physical or logical location
- Deployment and operational status
- Acquisition date and lifecycle or replacement information
- Funding source or grant designation where applicable.
- Disposal or transfer status

Asset Management

Technology assets must:

- Be tracked throughout their lifecycle.
- Be managed in accordance with security, operational, and compliance requirements.
- Remain subject to The Coalition monitoring, maintenance, audit, recovery, and disposal procedures.

Only authorized personnel may acquire, assign, transfer, reassign, or dispose of The Coalition technology assets. Such activities must be appropriately approved and documented.

Inventory Verification

The Coalition may periodically conduct and document physical inventory verification activities to confirm the existence, assignment, condition, and accuracy of technology asset records.

Missing, stolen, damaged, or unaccounted-for assets must be promptly reported, investigated, and documented in accordance with The Coalition procedures.

Unauthorized hardware, software, or technology devices may be restricted, removed, or disconnected from The Coalition systems.

IT160.02 Equipment Issuance and Tracking

Reference Procedure:

The Coalition technology equipment is issued to authorized users to support official business operations and job responsibilities.

Equipment Issuance

Technology equipment may include:

- Laptops and desktop computers
- Mobile phones and tablets
- Peripheral devices and accessories
- Security devices or authentication equipment
- Other approved technology resources

Equipment issuance must be:



- Authorized by management and/or CAO or Designee
- Recorded and tracked appropriately.
- Assigned to an identified user, department, or operational function.

User Responsibilities

Users issued The Coalition equipment are responsible for:

- Protecting equipment from theft, loss, damage, or misuse
- Using equipment in accordance with Coalition policies
- Promptly reporting lost, stolen, or damaged equipment
- Returning equipment upon request, role change, or separation

Technology assets always remain the property of the Coalition unless otherwise authorized in writing.

IT160.03 Maintenance and Support

Reference Procedure:

The Coalition maintains technology assets to support security, reliability, operational continuity, and lifecycle management.

Maintenance Activities

Authorized CAO or Designee or approved service providers may perform:

- Security updates and patching
- Hardware maintenance and replacement
- Software installation and support
- System monitoring and troubleshooting
- Configuration management and performance optimization

Authorized Support

Only authorized personnel may:

- Repair or modify Coalition Technology assets.
- Install software or hardware components.
- Configure administrative or security settings.
- Unauthorized maintenance, tampering, or modification of The Coalition systems or equipment is prohibited.

User Cooperation

Users are expected to:

- Cooperate with maintenance and support activities.
- Allow timely installation of required updates and security controls.
- Avoid interfering with monitoring, maintenance, or support processes.

Systems that present operational or security risks may be temporarily restricted, isolated, or removed from service.

IT160.04 Disposal of IT Equipment

Reference Procedure:



Coalition maintains secure disposal practices for technology assets and electronic media to protect confidential information and prevent unauthorized access to The Coalition data.

Disposal Requirements

Prior to disposal, transfer, recycling, or reassignment, technology assets must be reviewed to ensure that:

- The Coalition data is securely removed or destroyed.
- Storage media is sanitized in accordance with approved methods.
- Sensitive or restricted information cannot be recovered.

Covered Assets

Secure disposal requirements apply to:

- Computers and servers
- Mobile devices and tablets
- External storage devices and removable media
- Printers, copiers, and multifunction devices
- Networking equipment and other electronic storage technologies

Approved Disposal Methods

Disposal methods may include:

- Secure wiping or data sanitization
- Physical destruction of storage media
- Approved recycling or disposal services
- Return to authorized vendors or leasing providers.

Only authorized personnel or approved service providers may dispose of The Coalition technology assets.

Unauthorized disposal, transfer, sale, or removal of Coalition equipment or data is prohibited and may result in disciplinary or legal action.

IT170 – Vendor and Third-Party Management

IT170.01 – Vendor and Third-Party Management

Reference Procedure:

The Coalition may engage technology vendors, contractors, consultants, service providers, and other third parties to support operational and technology functions.

All third parties that access, store, process, transmit, or support The Coalition systems or data must:

- Be approved through an appropriate business and security review.
- Limit access to the minimum necessary for the authorized purpose.
- Protect Coalition data using reasonable administrative, technical, and physical safeguards.
- Follow The Coalition confidentiality, security, and acceptable use requirements.



- Promptly report suspected or actual security incidents involving The Coalition information.

Vendor access must be time-limited where practical, monitored as appropriate, and revoked when no longer needed or when the relationship ends. The Coalition may require confidentiality agreements, data protection agreements, or other contractual safeguards before access is granted.

IT170.02 Technology Vendor Selection

Reference Procedure:

The Coalition may engage technology vendors, contractors, consultants, service providers, and third-party partners to support operational, business, cybersecurity, and technology functions.

Vendor selection processes must consider operational needs, security requirements, compliance obligations, reliability, and risk to The Coalition systems and data.

Vendor Evaluation Criteria

- Technology vendors may be evaluated based on factors including:
- Business and operational requirements
- Information security and cybersecurity practices
- Ability to protect confidential or restricted information.
- Compliance with applicable laws, regulations, grant requirements, and contractual obligations
- Service reliability, support capabilities, and business continuity practices.
- Licensing, contractual, and financial considerations

Risk Considerations

Vendors that store, process, transmit, access, or support The Coalition systems or data may be subject to additional review based on:

- Type and sensitivity of information involved.
- Level of system or network access required.
- Operational dependency and criticality
- Regulatory, audit, or grant compliance requirements.

The Coalition reserves the right to approve, restrict, or deny vendor relationships that present unacceptable operational, cybersecurity, legal, or compliance risk.

IT170.03 Third-Party Security Requirements

Reference Procedure:

Third parties that access, process, store, transmit, manage, or support The Coalition systems or information must maintain appropriate security and confidentiality protections.

Security Expectations

Third parties may be required to:



- Maintain reasonable administrative, technical, and physical safeguards.
- Protect The Coalition data from unauthorized access, disclosure, alteration, or destruction.
- Comply with applicable legal, regulatory, contractual, and grant requirements.
- Follow The Coalition security requirements and acceptable use expectations.
- Promptly report actual or suspected security incidents involving The Coalition information or systems

Confidentiality and Data Protection

Third parties with access to confidential or restricted information may be required to:

- Execute confidentiality or data protection agreements.
- Limit access to authorized personnel with legitimate business need.
- Use approved secure transmission and storage methods.
- Return or securely destroy The Coalition information upon request or contract termination.

Security Reviews

The Coalition may:

- Request evidence of vendor security practices or compliance controls.
- Review vendor risk and security posture periodically.
- Restrict or terminate vendor access when security concerns are identified.

Failure to comply with Coalition security requirements may result in suspension or termination of vendor access, contractual remedies, or other corrective action.

IT170.04 Vendor System Access

Access to The Coalition systems, applications, networks, or data by vendors or third parties must be authorized, controlled, monitored, and limited to approved business purposes.

Access Authorization

Vendor access must:

- Be approved by authorized management and/or CAO or Designee
- Be limited to the minimum access necessary to perform authorized services.
- Be time-limited or project-based where appropriate.
- Be documented and subject to review.

Security Requirements

Third-party users granted system access must comply with:

- The Coalition IT and cybersecurity policies
- Access control and authentication requirements
- Multi-Factor Authentication (MFA) requirements where applicable
- Monitoring, logging, and audit controls

Shared accounts are prohibited unless specifically approved for operational necessity and adequately controlled.



Monitoring and Review

Vendor access may be:

- Logged, monitored, reviewed, and audited.
- Modified, restricted, or revoked at any time.
- Suspended immediately in response to security concerns, contract termination, or operational need.

Remote and Privileged Access

Remote access and privileged administrative access by vendors must be:

- Restricted to authorized personnel only.
- Secured using approved methods and encryption controls.
- Limited to approved maintenance, support, or operational activities

Unauthorized vendor access to The Coalition systems or information is prohibited.

IT180 – Policy Compliance and Enforcement

IT180.01 Monitoring and Enforcement

Reference Procedure:

Coalition monitors compliance with Information Technology (IT), cybersecurity, privacy, and data protection requirements to safeguard The Coalitional systems, information, operations, and regulatory obligations.

Compliance activities may include administrative, technical, operational, and security oversight measures designed to identify, prevent, and respond to unauthorized or inappropriate activity.

Monitoring Activities

Coalition reserves the right to monitor, review, audit, and evaluate:

- System and network activity
- User access and authentication activity
- Email, internet, and electronic communications.
- Data access, storage, transmission, and usage
- Device usage and endpoint activity
- Security logs, alerts, and monitoring systems
- Compliance with applicable policies, standards, and procedures

Monitoring may occur with or without notice, consistent with applicable laws, operational requirements, and security needs.

Enforcement Authority

The Coalition may take appropriate corrective or protective actions to:

- Protect systems, networks, and information resources.
- Address cybersecurity threats or operational risks.
- Enforce compliance with Coalition requirements.



- Investigate suspected violations, misuse, or unlawful activity.

Corrective actions may include:

- Restricting or revoking system access
- Isolating devices or accounts
- Conducting investigations or audits
- Requiring additional training or corrective measures
- Referring matters to law enforcement or regulatory authorities when appropriate

Users are required to cooperate with authorized investigations, audits, and compliance activities.

IT180.02 Violations

Reference Procedure:

Failure to comply with The Coalition IT policies, cybersecurity requirements, acceptable use standards, or data protection obligations may result in disciplinary or corrective action.

Policy Violations

Violations may include, but are not limited to:

- Unauthorized access to systems or information
- Sharing passwords or authentication credentials
- Circumventing security controls or monitoring systems
- Misuse of Coalition technology resources
- Failure to protect confidential or restricted information.
- Installation or use of unauthorized software, systems, or services
- Failure to report suspected security incidents or policy violations.
- Any activity that creates operational, legal, financial, cybersecurity, or reputational risk to the Coalition

Corrective and Disciplinary Actions

Depending on the nature and severity of the violation, the Coalition may take actions including:

- Verbal or written corrective action.
- Mandatory retraining or remediation
- Restriction, suspension, or revocation of access privileges
- Disciplinary action up to and including termination of employment or contract.
- Civil, contractual, financial, or legal remedies where applicable

The Coalition reserves the right to take immediate protective action when necessary to protect systems, data, operations, or compliance obligations.

IT180.03 Policy Acknowledgment

Reference Procedure:

All authorized users of The Coalition technology resources may be required to acknowledge and agree to comply with applicable IT policies, cybersecurity requirements, confidentiality obligations, and acceptable use standards.



Acknowledgment Requirements

Users may be required to acknowledge that they:

- Have received or been provided access to applicable policies and standards.
- Understand their responsibilities regarding system security and data protection.
- Agree to comply with Coalition technology and cybersecurity requirements.
- Understand that The Coalition systems may be monitored and audited.
- Understand that violations may result in disciplinary or legal consequences.

Timing of Acknowledgments

Acknowledgments may be required:

- Prior to receiving system access
- Upon implementation of policy or revision
- Periodically as part of compliance or training activities
- Following significant policy, security, or operational changes

Failure to complete required acknowledgments may result in delayed, restricted, suspended, or revoked access to Coalition systems and technology resources.

IT180.04 Exceptions and Risk Acceptance

Reference Procedure:

Exceptions to this policy may be granted only with written approval from Executive Leadership and, when appropriate, CAO or Designee.

An approved exception must:

- Identify the specific policy requirement being waived.
- State the business justification.
- Describe compensating controls, if any.
- Include an expiration date or review date.
- Be documented and retained for audit purposes.

Exceptions may be modified or revoked at any time if risk changes, compliance concerns arise, or operational needs require it.



Appendix A – Definitions

The following definitions apply to the Information Technology (IT) Policy Manual and associated standards, procedures, and supporting documentation.

Access Control

The process of granting, restricting, monitoring, and revoking access to systems, applications, networks, facilities, or data based on authorized business need.

Administrative Access

Elevated or privileged system access that allows configuration changes, user management, security administration, or control over systems or applications.

Approved System

Any technology system, application, platform, device, cloud service, or software authorized by the Coalition for The Coalitional use.

Asset

Any technology resource owned, leased, managed, or authorized by the Coalition, including hardware, software, cloud services, data, network infrastructure, mobile devices, and related equipment.

Audit Log

A record of system activity, access events, changes, or transactions maintained for operational, security, compliance, or investigative purposes.

Authentication

The process of verifying the identity of a user, system, or device before access is granted.

Authorization

Formal approval granting access, permissions, or authority to use The Coalition systems, data, or resources.

Backup

A secure copy of data, systems, or configurations maintained for recovery, restoration, continuity, or disaster recovery purposes.

Biometric Authentication

Identity verification based on physical or behavioral characteristics such as fingerprint, facial recognition, or other approved biometric methods.

Bring Your Own Device (BYOD)

The authorized use of personally owned devices to access The Coalition systems, networks, applications, or data.

Business Continuity



The capability of the Coalition to maintain or restore critical operations and services during or following a disruption.

Cloud Service

A hosted technology service, platform, infrastructure, or software solution provided over the internet or external network.

The Coalition Data

Any information created, received, stored, transmitted, processed, or maintained by the Coalition in any format.

Confidential Information

Sensitive information that is not publicly available and that could result in operational, legal, financial, reputational, or privacy harm if improperly disclosed.

Cybersecurity

The protection of systems, networks, devices, applications, and data from unauthorized access, misuse, disruption, destruction, or cyber threats.

Data Classification

The process of categorizing information according to sensitivity, confidentiality, regulatory requirements, and business impact.

Data Owner

The individual, department, or functional area responsible for oversight, classification, use, and protection of specific data or systems.

Device

Any electronic equipment capable of storing, transmitting, processing, or accessing The Coalition systems or data.

Encryption

A security method used to protect information by converting it into unreadable form unless properly decrypted using approved credentials or keys.

Endpoint

Any workstation, laptop, mobile device, server, or other device connected to or capable of connecting to The Coalition systems or networks.

Endpoint Detection and Response (EDR)

Security technology used to monitor, detect, investigate, and respond to suspicious or malicious activity on endpoint devices.

Firewall

A security control that monitors and filters network traffic to protect systems and networks from unauthorized access or malicious activity.

**Generative Artificial Intelligence (GenAI)**

Artificial intelligence technologies capable of generating text, images, code, audio, video, or other content based on prompts, data, or user input.

Incident

Any event that may compromise the confidentiality, integrity, availability, security, or proper operation of The Coalition systems, networks, devices, or information.

Information System

Any organized combination of hardware, software, networks, applications, data, people, and processes used to collect, store, process, transmit, or manage information.

Least Privilege

The security principle that users are granted only the minimum level of access necessary to perform authorized job responsibilities.

Malware

Malicious software designed to disrupt operations, damage systems, gain unauthorized access, or compromise information security.

Mobile Device

A portable computing or communication device includes smartphones, tablets, laptops, and similar technologies.

Multi-Factor Authentication (MFA)

An authentication method requiring two or more verification factors to confirm a user's identity.

Network

Connected systems, devices, applications, and communication infrastructure used to exchange or transmit data.

Network Segmentation

The separation of network environments or systems into controlled security zones to reduce unauthorized access and cybersecurity risk.

Personally Identifiable Information (PII)

Information that can identify, contact, or distinguish a specific individual either alone or when combined with other information.

Phishing

A fraudulent attempt to obtain sensitive information, credentials, or access through deceptive electronic communications.

Privileged Account

An account with elevated permissions capable of performing administrative, security, or high-risk system functions.

**Public Information**

Information approved for public release with no expected harm from disclosure.

Records Retention

The process of maintaining records and information for required legal, operational, regulatory, grant, or business time periods.

Remote Access

Authorized access to Coalition systems or networks from an external or offsite location.

Restricted / Highly Sensitive Information

Information requires the highest level of protection due to legal, regulatory, contractual, privacy, financial, operational, or security requirements.

Risk Assessment

The process of identifying, evaluating, and prioritizing operational, cybersecurity, privacy, or compliance risks.

Role-Based Access Control (RBAC)

An access management method where permissions are assigned according to standardized job roles or responsibilities.

Security Incident

Any actual, suspected, attempted, or confirmed event involving unauthorized access, misuse, disclosure, disruption, destruction, or compromise of systems or data.

Security Monitoring

The process of observing, reviewing, analyzing, and responding to system, network, or user activity for operational, security, or compliance purposes.

Sensitive Information

Information that requires protection from unauthorized disclosure, access, or misuse due to operational, legal, financial, privacy, or reputational considerations.

Social Engineering

Manipulation or deceptive tactics used to persuade individuals to disclose confidential information or perform unauthorized actions.

System Administrator

An authorized individual responsible for managing, configuring, securing, monitoring, or supporting information systems or technology infrastructure.

Technology Asset

Any hardware, software, application, cloud service, network component, storage media, mobile device, or technology resource used by the Coalition.

**Third Party**

Any external vendor, contractor, consultant, service provider, partner, volunteer, or non-The Coalition individual or entity authorized to access The Coalition systems, services, or information.

User

Any authorized individual who accesses, uses, manages, supports, or interacts with Coalition systems, devices, applications, networks, or information.

Virtual Private Network (VPN)

A secure encrypted connection used to access systems or networks remotely over public or external networks.

Vulnerability

A weakness, flaw, misconfiguration, or exposure that could be exploited to compromise the security or operation of systems or information.

Workstation

A desktop computer, laptop, or similar endpoint device used to access Coalition systems, applications, or information.

The Coalition may update, expand, or modify definitions periodically to reflect changes in technology, cybersecurity practices, legal requirements, operational needs, or applicable regulatory guidance.



Appendix B – References and IT Policy Mapping Matrix

This appendix combines:

1. Regulatory, legal, and standards-based references supporting the IT Policy Manual
2. A cross-reference mapping of IT100–IT180 policy sections to applicable frameworks and laws

This combined structure is intended to support audit readiness, grant compliance, cybersecurity governance, and policy traceability.

PART I – REFERENCES

Federal Laws and Regulations

- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g
- Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160 and 164 (if applicable)
- Federal Information Security Modernization Act (FISMA)
- Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (as applicable)
- Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (as applicable)
- U.S. Copyright Law, Title 17, United States Code

State of Florida Laws and Regulations

- Florida Information Protection Act (FIPA), Section 501.171, Florida Statutes
- Florida Public Records Law, Chapter 119, Florida Statutes
- Florida Computer Crimes Act, Section 815.06, Florida Statutes
- Florida Cybersecurity Standards and Governance Requirements, Chapter 60GG-2, Florida Administrative Code
- Florida Records Retention Schedules, GS1-SL (State and Local Government Agencies)
- Applicable Florida Department of Education / Division of Early Learning requirements

Florida Department of Education / Division of Early Learning Guidance

- DEL Program Guidance 240.02 – Property and Equipment Inventory Requirements
- DEL Program Guidance 300.01 – Information Technology Security Manual (legacy reference)
- State-funded early learning grant agreements and contractual requirements

Security Frameworks and Industry Standards

- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 – Security and Privacy Controls
- NIST SP 800-61 – Incident Handling Guide
- NIST SP 800-63 – Digital Identity Guidelines
- NIST SP 800-34 – Contingency Planning
- NIST SP 800-40 – Patch Management
- NIST SP 800-41 – Firewalls and Network Security
- NIST SP 800-46 – Telework Security



- NIST SP 800-88 – Media Sanitization
- NIST AI Risk Management Framework (AI RMF 1.0)
- CIS Critical Security Controls
- ISO/IEC 27001 Information Security Management Systems

Grant and Financial Compliance Requirements

- Uniform Guidance (2 CFR Part 200)
- State of Florida DOE grant agreements (School Readiness, VPK, and related programs)
- Vendor and subcontractor contractual obligations

PART II – IT POLICY MAPPING MATRIX (IT100–IT180)

This matrix maps IT policy sections to applicable legal, regulatory, and standards-based frameworks.

IT100 – IT Governance and Administration

IT100.01–IT100.06

- NIST CSF
- NIST SP 800-53
- Florida Cybersecurity Standards (60GG-2 FAC)
- FIPA §501.171
- 2 CFR Part 200
- DOE / DEL contractual requirements

IT110 – Information Security

IT110.01 Security Governance

- NIST CSF
- NIST SP 800-53
- CIS Controls
- Florida Cybersecurity Standards

IT110.02 Data Classification

- FIPA §501.171
- FERPA
- NIST SP 800-53
- CIS Controls

IT110.03 Identity & Access Management

- NIST SP 800-63
- NIST SP 800-53
- CIS Controls

IT110.04 Security Operations

- NIST SP 800-53
- NIST SP 800-61
- CIS Controls

IT110.05 Incident Response

- NIST SP 800-61
- NIST CSF



- FIPA breach requirements

IT110.06 Remote Access

- NIST SP 800-46
- NIST SP 800-53

IT120 – User Access Management

- NIST SP 800-63
- NIST SP 800-53
- CIS Controls
- FIPA

IT130 – Network and System Security

IT130.01 Network Security

- NIST SP 800-53
- CIS Controls

IT130.02 Firewalls

- NIST SP 800-41

IT130.03 System Hardening

- CIS Benchmarks
- NIST SP 800-53

IT130.04 Patch Management

- NIST SP 800-40
- CIS Controls

IT130.05 Endpoint Security

- NIST SP 800-53
- CIS Controls

IT130.06 BYOD

- NIST SP 800-124
- CIS Controls

IT130.07 Mobile Security

- NIST SP 800-124
- FIPA

IT130.08 Physical Security

- NIST SP 800-53 (PE controls)
- CIS Controls

IT140 – Data Management and Protection

IT140.01 Data Retention

- Chapter 119, Florida Statutes
- GS1-SL Records Schedule
- 2 CFR Part 200

IT140.02 Data Storage

- NIST SP 800-53
- CIS Controls

IT140.03 Backup and Restoration

- NIST SP 800-34

IT140.04 Data Recovery



- NIST SP 800-34

IT140.05 Records Retention / Legal Hold

- Chapter 119, F.S.
- 2 CFR Part 200

IT150 – Acceptable Use and Communications

IT150.01 Email Use

- FIPA
- NIST CSF

IT150.02 Monitoring

- NIST SP 800-53
- FIPA

IT150.03 Security Awareness

- NIST CSF
- CIS Controls

IT150.04 User Training

- NIST CSF
- CIS Controls

IT150.05 GenAI Use

- NIST AI RMF
- FIPA
- U.S. Copyright Law

IT150.06 Social Media

- NIST CSF
- FIPA
- NLRA considerations

IT160 – Technology Assets

IT160.01 Inventory

- DEL 240.02
- 2 CFR Part 200
- NIST SP 800-53
- CIS Controls

IT160.02 Equipment Tracking

- 2 CFR Part 200

IT160.03 Maintenance

- NIST SP 800-53

IT160.04 Disposal

- NIST SP 800-88
- 2 CFR Part 200
- FIPA

IT170 – Vendor Management

- 2 CFR Part 200
- NIST SP 800-53
- CIS Controls
- FIPA



IT180 – Compliance and Enforcement

IT180.01 Monitoring

- NIST SP 800-53
- FIPA

IT180.02 Violations

- FIPA
- NIST CSF

IT180.03 Acknowledgment

- 2 CFR Part 200

IT180.04 Exceptions

- NIST Risk Management Framework (RMF)

Summary

This combined appendix establishes a unified reference and traceability framework linking The Coalition IT policy requirements to:

- Federal law
- Florida statutes and cybersecurity requirements
- Florida Department of Education / DEL guidance
- NIST, CIS, and ISO security frameworks
- Grant and contractual obligations

The Coalition may update this appendix as legal, regulatory, cybersecurity, and operational requirements evolve.

Action Items

Early Learning Coalition of Marion County Meeting Minutes

Meeting: Full Coalition Board Meeting

Date/Time: August 27, 2026; 8:30 AM

Location: ELCMC Office, 2300 SW 17th Road, Ocala, FL 34471/Via Conference Call

Attendance –

Present (In-Person): Todd Panzer, Thomas LoBianco, Jennifer Beck, Kim LaCognata, Dr. Kim Sellers, Lola Gonzalez, Jessica Schultz, Cecil Wilson, Shannon Mills, Richard Forrester, Commissioner Matthew McClain, Heather Gamble

Present (Virtual): Levonda Goodson, Jennifer McBride, Maritza Alejandro

Absent (Excused): Brenda Ford, Christy Jergens, Jennifer Winton

Absent (Un-Excused): Brittney Morley

Guest (Virtual): Gemma Torcivia and Kate Watson; TG Law PLLC

Staff Present: LaTrisha Sims, Chief Executive Officer; Elizabeth Deola, CPO; Marcelle Easter, CAO; Beatriz Montalvo, HR Director; Dr. Michelle Grant Harris, Wendy Williams, Community Relations Director; Michelle Eurbín, Family Services Director; Josef Izquierdo, Data Integrity Coordinator II; Zack Hackley, Finance Consultant

Agenda Item	Summary/Discussion	Action
Call to Order Roll Call	Todd Panzer called the meeting to order. Beatriz Montalvo called roll. Quorum was present.	The meeting was called to order at 8:32 AM.
Sunshine Law & Ethics Training	Gemma Torcivia and Kate Watson from TG Law PLLC covered the Sunshine Law & Ethics training. Article I, Section 24 of the Florida Constitution establishes the constitutional right of public access to government records and meetings (often called Florida's "Sunshine Law").	
2026 – 2027 Budget R-1	M. Easter presented the FY 2026-2027 Budget, Revision-1, in detail. ELCMC received level funding. DEL revised the allocation process for quality differentials, including Quality Performance Initiative, Gold Seal Accreditation, and Special Needs Rate funding, which will now be allocated in six-month increments. Insurance costs decreased by approximately \$14,000 following a policy change, with the savings reallocated to software. Discussion included the DEL June invoice, an estimated \$50 rollover, and the potential impact of the state's reversion process.	RATIFICATION: Executive Committee moved to accept the budget revision as presented on August 6, 2026. L. Gonzalez second. Motioned passed unanimously.
Bylaws	L. Sims asked to approve the changes to the ELCMC Bylaws as requested by DEL to ensure compliance with section 1002.83, Florida Statutes and authorize submission	RATIFICATION: Executive Committee moved to accept the Bylaws revision as

	to the revised Bylaws and associated plan amendment request to DEL. The resubmission due date was August 14, 2026.	presented on August 6, 2026. K. LaCognata second. Motioned passed unanimously.
Board Member Resignation & Appointment	The ELCMC was notified on July 8, 2026, that Telisha Page was no longer employed by DCF and therefore could no longer serve as the Local DCF Regional Administrator Designee on the ELCMC Board of Directors. DCF subsequently designated Jamie Blunt to serve in her place. The Local DCF Regional Administrator Designee is a mandated position on the ELCMC Board of Directors under Florida Statutes and the ELCMC Bylaws.	RATIFICATION: Executive Committee moved to accept the Board member resignation and appointment as presented on August 6, 2026. L. Gonzalez second. Motioned passed unanimously.
Board Membership Gubernatorial End Dates	L. Sims asked to approve the ELCMC Board Membership Roster. DEL has provided directives to add the current term length, current term end date, and current term number dates to the document. The updated roster was due for submission to DEL by August 14, 2026.	RATIFICATION: Executive Committee moved to accept the Board membership gubernatorial end dates as presented on August 6, 2026. K. LaCognata second. Motioned passed unanimously.
Full Coalition Board Meeting Minutes	June 25, 2026, Full Coalition Board minutes were included in the packet for review and approval. No changes were recommended.	ACTION: Dr. K. Sellers moved to accept the minutes as presented. L. Goodson second. Motioned passed unanimously.
Financials through May 2026	Zack Hackley presented the ELCMC financial reports through May 2026. - Zack Hackley presented the ELCMC financial reports through May 2026. All cash accounts were reconciled as of May 31, with approximately \$986,000 in cash, \$2.021 million in accounts receivable (including \$1.961 million due from DEL), \$1.633 million in current accounts payable, and \$1.299 million due to DEL. Total net assets were approximately \$522,000. The Income Statement was reviewed. All state budgetary mandates are being met: - School Readiness (SR) Direct Service – Required: 78% ELCMC Actual: 79.6% - SR Admin – Required: <5% ELCMC Actual: 3.63% - SR Admin/Non-Direct/Quality – Required: 22% Max ELCMC Actual: 19.7% - SR Quality – Required: 4% Min ELCMC Actual: 8.4% - Voluntary Pre-Kindergarten (VPK) Admin – Required: 5% Max ELCMC Actual: 4.392% - SR Plus Admin – Required: 5% Max ELCMC Actual: 0.3%	ACTION: Executive Committee moved to accept financials as presented on August 6, 2026. K. LaCognata second. Motioned passed unanimously.
Board Member Nomination	L. Sims asked to approve the nomination of Heather Gamble as a Private Sector Representative for a four-year	ACTION: T. LoBianco moved to accept the Board

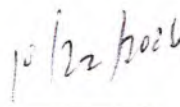
	term beginning on August 27, 2026, through June 30, 2030.	nomination as presented. J. Beck second. Motioned passed unanimously.
CEO Update –	L. Sims shared several updates including: • Kiwanis awarded ELCMC \$1,125 for children's books, and the Community Foundation awarded \$1,000 toward grant writing for early literacy initiatives. • Community diaper drives continue to provide donations. • DEL Chancellor Carrie Miller resigned; Katerina Maroney is serving as interim Chancellor. • SR enrollment increased by 156 children from May to June; 2,363 children enrolled for SR, internal projection is 2,500. • VPK enrollment is down statewide by approximately 7,000 students. The state estimates 1,586 VPK enrollments in Marion County; ELCMC currently has 2,300 children approved with certificates of eligibility and is working to exceed the estimate. • ELCMC is increasing outreach efforts and developing a Kindergarten Transition Plan. • ELCMC requested \$150,000 in County match funding and \$25,000 for DPIL. Due to uncertainty surrounding county funding and tax reductions, ELCMC was referred to CDBG. Failure to secure eligible match funds could result in \$300,000 in total funding being de-obligated from the ELCMC budget. • ELCMC is allowing natural attrition in the Dolly Parton's Imagination Library program while seeking additional funding and exploring other early literacy programs. We've received donations in lieu of flowers. • Thank you to all who assisted with the distribution of calendars.	ELCMC Information
Give4Marion Goals	W. Williams shared the goals for this year's Give 4 Marion Campaign as outlined in the packet. The goal set for the Board is to achieve 100% giving/participation, historically, have received 90% giving/participation over past two years. ELCMC is hosting after-hours Peer to Peer friend raising. ELCMC cannot use state dollars to fundraise, so all campaign participation is done off-the-clock, after hours, and voluntarily.	ELCMC Information
4 th Quarter Impact Report	W. Williams discussed the 4 th Quarter Impact Report included in the packet for informational purposes.	ELCMC Information
College of Central Florida	Dr. K. Sellers shared the following highlights: • Enrollments are up. • The College of Central Florida and MCPS presented the 2026 Careers and Colleges Expo last night. Had attendees as young as middle school age.	Community Roundtable

	The Learning Lab School was privileged to have M. Maysonet and Dr. M. Grant Harris present the Above the Line training. It was amazing!	
Preschool @ The Springs	K. LaCognata shared an impactful experience a parent had through the Incredible Years program.	Community Roundtable
CEP	J. Schultz asked for positive thoughts and prayers during the hiring process for the Director of South Marion. Belleview after hours will be held tonight. All are welcome to attend.	Community Roundtable
Mortgages with Brittany	H. Gamble is thankful for the opportunity to serve on the ELCMC Full Coalition Board of Directors. She's happy to be here.	Community Roundtable
Mary's Family Childcare, Inc.	C. Wilson shared that CDS is closing their food program.	Community Roundtable
Marion County School Board	J. Beck shared the following highlights: 21 of the 35 scored the highest on the VPK Performance Metrics. - VPK classes should be 100% full by next week. 675 at 33 sites – 135 IEP and inclusive settings	Community Roundtable
ELCMC	W. Williams shared the following updates: BJ's Club Membership – A BJ's flyer was distributed with a UR code to help support ELCMC "for a Cause".	Community Roundtable
2026 – 2027 Early Learning Sponsorship Opportunities	The 2026 – 2027 Early Learning Sponsorship Opportunities flyer was distributed for informational purposes.	Information Item
Upcoming Events	Upcoming meeting dates were included on the agenda for planning purposes.	Information Item
Public Comment	None at this time.	
Adjournment	Meeting adjourned at 10:10 AM.	T. Panzer motioned to adjourn the meeting.

Reported by: Beatriz Montalvo, HR Director

Approved by: _____

Todd Panzer, Chair

Date: _____


NOTE: For additional information on any of the above items, please contact LaTrisha Sims, Chief Executive Officer at lsims@elc-marion.org.

ELC of Marion County

Reporting on July 31, 2026 Financial Statements

Fiscal year 2026-2027

Finance Notes:

Tick marks below correspond to the matching tick marks on the attached July 31, 2026 Balance Sheet, Income Statement – All Funds, and the SR and VPK fund-level Income Statements.

Balance Sheet:

- **(a)** All cash accounts (Operating, Unrestricted, Building, PayPal, Community Foundation, and petty cash) have been reconciled as of July 31, 2026. Currently we are holding approximately \$1,350,000 in cash. Cash naturally fluctuates with the timing of the FOEL reimbursement draw cycle — balances dip as expenditures are paid out and build back up as reimbursement is received.
- **(b)** Accounts receivable consists of approximately \$2,300,000, of which approximately \$2,244,000 is due from FOEL. The balance reflects invoices to DEL that remain outstanding for the most recent months. See AR Aging Schedule.
- **(c)** We have fixed assets with a net book value of approximately \$520,000 (shown as “Other” on the balance sheet).
- **(d)** Accounts payable consists of approximately \$1,475,000 and is current.
- **(e)** Due to DEL (Payable: FOEL Advance) is approximately \$2,308,000.
- **(f)** Total Net Assets is approximately \$273,000.

Income Statement – All Funds

- **(1)** Grant Revenues have increased year over year, from \$1,561,114 to \$1,788,010 (+\$226,895), due to serving more kids.
- **(2)** Salaries (Personnel Expenses) have increased year over year, from \$206,475 to \$304,739 (+\$98,264), due to 3 payroll cycles in July 2026.
- **(3)** Program Expenses are up year over year, from \$1,199,153 to \$1,442,921 (+\$243,768), due to higher enrollment.
- **(4)** Maintenance and Repairs decreased year over year, from \$42,012 to \$2,641 (-\$39,372), due to general liability insurance being classified under this category in the prior year. All other insurance is classified under miscellaneous. Miscellaneous expense is up from \$7,618 to \$55,566 (+\$47,948)
- **(5)** (see SR Income Statement) SR Program Expenses are up year over year, from \$1,145,947 to \$1,372,544 (+\$226,598), consistent with increased child enrollment.
- **(6)** (see VPK Income Statement) VPK Program Expenses (direct services) are up slightly year over year, from \$46,400 to \$70,376 (+\$23,977), due to serving few more VPK-eligible children this year compared to last year. As always, we serve all children who are four years old and want to attend, regardless of funding.

Dashboard mandates:

SR Admin = 4.23%

SR Direct Services = 72.8% Under the 78% mandate

Quality = 10.4%

VPK Admin = 30.06% Over the 5% maximum

Early Learning Coalition of Marion County, Inc.

Balance Sheet
As of 7/31/2026
(In Whole Numbers)

Current Year

Assets

Cash: Operating (0332)	1,098,756	A
Cash: Unrestricted (0340)	130,093	
Cash: Building (0464)	30,301	
Cash: PayPal	317	
Cash: Community Foundation	128,166	
Petty Cash: Vending Machine	61	
Petty Cash: Outreach	(10)	B
A/R: FOEL	2,284,598	
A/R: Other Grants	10,529	
A/R: Overpayments	1,061	
Due from Employee	(25)	
A/R: Clearing	23,432	
Prepaid: Postage	1,111	C
Prepaid: Other	15,721	
Prepaid: Travel Advance	2,150	
Other	519,638	
Total Assets	4,245,900	

Liabilities

Credit Card (South State - VISA)	768	D
Accounts Payable	1,496,011	
A/P: Conversion	(25,986)	
Payable: Accrued PLT	114,855	
Payable: Medicare	(0)	
Payable: SUTA	(36)	
Payable: Health Insurance	(20,727)	E
Payable: Dental Insurance	22	
Payable: Vision Insurance	1,906	
Payable: ER - 403(b)	(1,609)	
Payable: EE - 403(b)	11,766	
Payable: EE - Roth IRA	1,130	
Payable: Life Insurance	165	F
Payable: Short-term Disability	285	
Payable: Long-term Disability	(766)	
Payable: AFLAC	1,892	
Payable: Colonial Life	(256)	
Payable: United Way Deductions	10,933	
Payable: Wage Garnishment	532	E
Payable: Workers Compensation	(1,311)	
Payable: FOEL Advance	2,308,081	
2701: A/R: VPPRP VPK Provider Advance	(3,811)	
Payable: Interest	1,655	
Payable: Fraud Collections	24,322	
Deferred Revenue	52,960	F
Total Liabilities	3,972,781	

Net Assets 273,119 F

Total Liabilities and Net Assets 4,245,900

Early Learning Coalition of Marion County, Inc.

Aged Receivables by Invoice Date
Aging Date - 7/31/2026
From 7/1/2025 Through 7/31/2026

Customer ID	Customer Name	Invoice Date	Invoice Number	Description	Total	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due
Children's Forum	Children's Forum , Inc - HMG	7/20/2026	25hmgfa-12812	JUNE HMG INV	28,736.10	0.00	28,736.10	0.00	0.00	0.00
Children's Forum		8/21/2026	26HMGFA-12R31	JUL HMG INV	11,808.29	11,808.29	0.00	0.00	0.00	0.00
Total Children's Forum	Children's Forum , Inc - HMG				40,544.39	11,808.29	28,736.10	0.00	0.00	0.00
FOEL	Florida's Office of Early Learning	6/30/2026	3270726S1	FOEL JULY SPCL INV	107,168.83	0.00	0.00	107,168.83	0.00	0.00
FOEL		7/27/2026	3260626R1	FOEL JUNE INV	136,372.59	0.00	136,372.59	0.00	0.00	0.00
FOEL		7/31/2026	3270726R1	FOEL JULY 2026 INV	2,000,512.50	2,000,512.50	0.00	0.00	0.00	0.00
Total FOEL	Florida's Office of Early Learning				2,244,053.92	2,000,512.50	136,372.59	107,168.83	0.00	0.00
Joan S. Hatten	Joan S. Hatten	6/30/2021	FY19SR-J.S.Hatten	Joan S. Hatten 2018 - 2019 - Overpayment SR Recon	1,061.26	0.00	0.00	0.00	0.00	1,061.26
Total Joan S. Hatten	Joan S. Hatten				1,061.26	0.00	0.00	0.00	0.00	1,061.26
MCBOCC	Marion County Board of County Commissioners	9/30/2022	082022MCMA	MCBOCC - Match - September 2022	(39.96)	0.00	0.00	0.00	0.00	(39.96)
MCBOCC		6/30/2024	062024MCMA	MCBOCC- MATCH- June 2024	0.03	0.00	0.00	0.00	0.00	0.03
MCBOCC		1/31/2025	0125DPL	DPIL Early Literacy Assistance FY24-25	2,349.79	0.00	0.00	0.00	0.00	2,349.79
MCBOCC		2/27/2026	0126DPL	DPIL ELA Assistance FY 26 - Jan 2026	(0.03)	0.00	0.00	0.00	0.00	(0.03)
Total MCBOCC	Marion County Board of County Commissioners				2,309.83	0.00	0.00	0.00	0.00	2,309.83

Early Learning Coalition of Marion County, Inc.

Aged Receivables by Invoice Date
Aging Date - 7/31/2026
From 7/1/2025 Through 7/31/2026

Customer ID	Customer Name	Invoice Date	Invoice Number	Description	Total	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due
SBMC	The School Board of Marion County, Florida	12/18/2025	YPP-1125	YPP Invoices	1,780.37	0.00	0.00	0.00	0.00	1,780.37
SBMC		5/19/2026	YPP-0126b	YPP RECONCILIATIO... INVOICES 25-26	1,477.67	0.00	0.00	0.00	1,477.67	0.00
SBMC		5/19/2026	ypp-0925b	YPP RECONCILIATIO... INVOICES 25-26	165.92	0.00	0.00	0.00	165.92	0.00
SBMC		5/19/2026	YPP-1125b	YPP RECONCILIATIO... INVOICES 25-26	191.22	0.00	0.00	0.00	191.22	0.00
SBMC		5/19/2026	YPP-1225b	YPP RECONCILIATIO... INVOICES 25-26	1,045.25	0.00	0.00	0.00	1,045.25	0.00
SBMC		5/21/2026	YPP-0825b	YPP RECONCILIATIO... INVOICES 25-26	163.30	0.00	0.00	0.00	163.30	0.00
SBMC		6/29/2026	YPP-0526	YPP-0526	<u>3,395.53</u>	<u>0.00</u>	<u>0.00</u>	<u>3,395.53</u>	<u>0.00</u>	<u>0.00</u>
Total SBMC	The School Board of Marion County, Florida				8,219.26	0.00	0.00	3,395.53	3,043.36	1,780.37
UWMC	United Way of Marion County, Inc.	6/1/2026	202606-UW	United Way Invoice - JUN 2026	(0.01)	0.00	0.00	(0.01)	0.00	0.00
Total UWMC	United Way of Marion County, Inc.				<u>(0.01)</u>	<u>0.00</u>	<u>0.00</u>	<u>(0.01)</u>	<u>0.00</u>	<u>0.00</u>
Report Total					<u>2,296,188.65</u>	<u>2,012,320.79</u>	<u>165,108.69</u>	<u>110,564.35</u>	<u>3,043.36</u>	<u>5,151.46</u>

Early Learning Coalition of Marion County, Inc.
Aged Payables by Due Date - Zh AP Aging Report - All Funds
Aging Date - 7/31/2026
From 7/1/2025 Through 7/31/2026

Vendor Name	Invoice Number	Invoice/Cre... Date	Due Date	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due	Total
Together For Children Inc	030219-593565606-... tfc	7/1/2019 6/30/2025	7/31/2019 7/30/2025	0.00 <u>0.00</u>	0.00 <u>0.00</u>	0.00 <u>0.00</u>	0.00 <u>0.00</u>	0.04 <u>(0.04)</u>	0.04 <u>(0.04)</u>
Total Together For Children Inc				0.00	0.00	0.00	0.00	0.00	0.00
Tonika's Home Child Care	SR0726-3846-27526	7/31/2026	8/21/2026	<u>1,015.32</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>1,015.32</u>
Total Tonika's Home Child Care				1,015.32	0.00	0.00	0.00	0.00	1,015.32
Triumphant Tots, Inc	SR0726-262794334-...	7/31/2026	8/21/2026	<u>3,275.33</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>3,275.33</u>
Total Triumphant Tots, Inc				3,275.33	0.00	0.00	0.00	0.00	3,275.33
Verizon Wireless	913502808-00004-01	5/30/2023	6/8/2023	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>(968.28)</u>	<u>(968.28)</u>
Total Verizon Wireless				0.00	0.00	0.00	0.00	(968.28)	(968.28)
Walmart	V-012023-C	2/2/2023	2/2/2023	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>15.00</u>	<u>15.00</u>
Total Walmart				0.00	0.00	0.00	0.00	15.00	15.00
West Family Learning Center East, LLC	0626-SY01-6656-000 SR0726-811326656-...	7/31/2026 7/31/2026	8/21/2026 8/21/2026	857.56 <u>12,154.35</u>	0.00 <u>0.00</u>	0.00 <u>0.00</u>	0.00 <u>0.00</u>	0.00 <u>0.00</u>	857.56 <u>12,154.35</u>
Total West Family Learning Center East, LLC				13,011.91	0.00	0.00	0.00	0.00	13,011.91
Wilma Martin Family Daycare Home	0526-SY01-8920-000 0626-SY01-8920-000 SR0726-882898920-...	7/31/2026 7/31/2026 7/31/2026	8/21/2026 8/21/2026 8/21/2026	75.00 479.13 <u>10,624.91</u>	0.00 0.00 <u>0.00</u>	0.00 0.00 <u>0.00</u>	0.00 0.00 <u>0.00</u>	0.00 0.00 <u>0.00</u>	75.00 479.13 <u>10,624.91</u>
Total Wilma Martin Family Daycare Home				11,179.04	0.00	0.00	0.00	0.00	11,179.04
Wilson's Lovable Daycare, LLC	SR0726-825414548-...	7/31/2026	8/21/2026	<u>10,255.87</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>10,255.87</u>
Total Wilson's Lovable Daycare, LLC				10,255.87	0.00	0.00	0.00	0.00	10,255.87
Wiz Kids Learning Academy	SR0726-472528160-...	7/31/2026	8/21/2026	<u>21,337.68</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>0.00</u>	<u>21,337.68</u>
Total Wiz Kids Learning Academy				21,337.68	0.00	0.00	0.00	0.00	21,337.68
Report Total				<u>1,472,145.04</u>	<u>24,332.32</u>	<u>6,512.39</u>	<u>(1,356.96)</u>	<u>(5,621.50)</u>	<u>1,496,011.29</u>

Early Learning Coalition of Marion County, Inc.

Statement of Revenues and Expenditures - Detail

From 7/1/2026 Through 7/31/2026

	Current Period Actual	Prior Year Current Period Actual	Current Period Change	
Operating Revenue				
Grant Revenue	1,788,009.93	1,561,113.95	226,895.98	1
Contributions	1,069.32	503.61	565.71	
Program Revenue	280.00	0.00	280.00	
Investment Income	364.63	248.90	115.73	
Total Operating Revenue	<u>1,789,723.88</u>	<u>1,561,866.46</u>	<u>227,857.42</u>	
Total Revenue	<u>1,789,723.88</u>	<u>1,561,866.46</u>	<u>227,857.42</u>	
Expenditures				
Personnel Expenses	304,739.03	206,474.79	98,264.24	2
Program Expenses	1,442,920.70	1,199,152.65	243,768.05	3
Professional Fees	11,592.00	4,528.56	7,063.44	
Supplies	37.18	2,077.58	(2,040.40)	
Telephone	1,522.91	2,032.82	(509.91)	
Postage & Shipping	80.34	33.30	47.04	
Occupancy	5,898.73	6,167.15	(268.42)	
Maintenance & Repairs	2,640.58	42,012.80	(39,372.22)	4
Equipment Rental	0.00	270.12	(270.12)	
Conferences, Conventions & Meetings	325.00	750.00	(425.00)	
Printing & Publications	891.79	1,494.32	(602.53)	
Dues & Subscriptions	6,325.00	6,100.00	225.00	
Depreciation	2,223.15	2,223.15	0.00	
Miscellaneous	55,566.17	7,617.93	47,948.24	4
Total Expenditures	<u>1,834,762.58</u>	<u>1,480,935.17</u>	<u>353,827.41</u>	
Net Revenue Over Expenditures	<u>(45,038.70)</u>	<u>80,931.29</u>	<u>(125,969.99)</u>	

Early Learning Coalition of Marion County, Inc.

Statement of Revenues and Expenditures - Detail

From 7/1/2026 Through 7/31/2026

	Current Period Actual	Prior Year Current Period Actual	Current Period Change
Operating Revenue			
Grant Revenue	<u>1,714,069.51</u>	<u>1,456,006.22</u>	<u>258,063.29</u>
Total Operating Revenue	<u>1,714,069.51</u>	<u>1,456,006.22</u>	<u>258,063.29</u>
Total Revenue	<u>1,714,069.51</u>	<u>1,456,006.22</u>	<u>258,063.29</u>
Expenditures			
Personnel Expenses	276,016.31	280,591.02	(4,574.71)
Program Expenses	1,372,544.42	1,145,946.84	226,597.58
Professional Fees	10,621.50	3,958.94	6,662.56
Supplies	36.55	475.96	(439.41)
Telephone	1,483.15	1,422.98	60.17
Postage & Shipping	78.44	10.28	68.16
Occupancy	5,744.78	5,276.81	467.97
Maintenance & Repairs	2,571.64	29,408.96	(26,837.32)
Conferences, Conventions & Meetings	300.00	750.00	(450.00)
Printing & Publications	868.51	1,461.23	(592.72)
Dues & Subscriptions	6,250.00	6,025.00	225.00
Depreciation	514.35	0.00	514.35
Miscellaneous	<u>53,137.77</u>	<u>5,238.74</u>	<u>47,899.03</u>
Total Expenditures	<u>1,730,167.42</u>	<u>1,480,566.76</u>	<u>249,600.66</u>
Net Revenue Over Expenditures	<u>(16,097.91)</u>	<u>(24,560.54)</u>	<u>8,462.63</u>

Early Learning Coalition of Marion County, Inc.

Statement of Revenues and Expenditures - Detail

From 7/1/2026 Through 7/31/2026

	Current Period Actual	Prior Year Current Period Actual	Current Period Change
Operating Revenue			
Grant Revenue	<u>62,132.13</u>	<u>78,796.08</u>	<u>(16,663.95)</u>
Total Operating Revenue	<u>62,132.13</u>	<u>78,796.08</u>	<u>(16,663.95)</u>
Total Revenue	<u>62,132.13</u>	<u>78,796.08</u>	<u>(16,663.95)</u>
Expenditures			
Personnel Expenses	16,555.11	21,225.18	(4,670.07)
Program Expenses	70,376.28	46,399.71	23,976.57
Professional Fees	158.96	569.62	(410.66)
Supplies	0.63	93.45	(92.82)
Telephone	39.76	609.84	(570.08)
Postage & Shipping	1.90	0.00	1.90
Occupancy	153.95	890.34	(736.39)
Maintenance & Repairs	68.94	12,603.84	(12,534.90)
Printing & Publications	23.28	33.09	(9.81)
Depreciation	99.73	0.00	99.73
Miscellaneous	<u>1,160.40</u>	<u>139.37</u>	<u>1,021.03</u>
Total Expenditures	<u>88,638.94</u>	<u>82,564.44</u>	<u>6,074.50</u>
Net Revenue Over Expenditures	<u>(26,506.81)</u>	<u>(3,768.36)</u>	<u>(22,738.45)</u>

6

Early Learning Coalition of Marion County, Inc.

Normal Trial Balance - TB ZH

From 7/1/2026 Through 7/31/2026

Account Code	Account Title	Debit Balance	Credit Balance
1000	Cash: Operating (0332)	1,098,756.32	
1010	Cash: Unrestricted (0340)	130,092.68	
1020	Cash: Building (0464)	30,300.95	
1050	Cash: PayPal	316.54	
1080	Cash: Community Foundation	128,166.08	
1091	Petty Cash: Vending Machine	60.74	
1092	Petty Cash: Outreach		10.00
1095	Credit Card (VISA)	0.00	
1096	Credit Card (MasterCard)	0.00	
1097	Credit Card (Sam's Club)	0.00	
1098	Credit Card (South State - VISA)		767.58
1200	A/R: FOEL	2,284,598.31	
1210	A/R: Other Grants	10,529.08	
1220	A/R: Overpayments	1,061.26	
1290	Due from Employee		24.92
1299	A/R: Clearing	23,432.49	
1400	Prepaid: Postage	1,111.08	
1401	Prepaid: Insurance	0.00	
1403	Prepaid: Other	15,720.79	
1405	Prepaid: Travel Advance	2,150.05	
1500	Fixed Assets: Equipment	58,707.26	
1501	Fixed Assets: Furniture	5,300.00	
1502	Fixed Assets: Building	856,517.59	
1503	Fixed Assets: Land	116,960.14	
1600	Accumulated Depreciation: Equipment		58,707.10
1601	Accumulated Depreciation: Furniture		5,300.00
1602	Accumulated Depreciation: Building		453,839.62
2000	Accounts Payable		1,496,011.29
2099	A/P: Conversion	25,985.97	
2100	Notes Payable: LOC	0.00	
2105	Notes Payable: HVAC	0.00	
2200	Payable: Salary	0.00	
2203	Payable: Accrued PLT		114,855.32
2205	Payable: Social Security	0.00	
2206	Payable: Medicare	0.39	
2207	Payable: SUTA	35.68	
2208	Payable: Federal Withholding	0.00	
2210	Payable: Health Insurance	20,727.03	
2211	Payable: Dental Insurance		21.74
2212	Payable: Vision Insurance		1,906.31
2213	Payable: HSA	0.00	
2220	Payable: ER - 403(b)	1,609.41	
2221	Payable: EE - 403(b)		11,766.24
2222	Payable: EE - Roth IRA		1,130.00
2230	Payable: Life Insurance		165.15
2231	Payable: Short-term Disability		284.62
2232	Payable: Long-term Disability	766.33	
2240	Payable: AFLAC		1,891.60
2245	Payable: Colonial Life	255.52	
2250	Payable: United Way Deductions		10,933.40
2255	Payable: Wage Garnishment		531.54
2265	Payable: Workers Compensation	1,310.78	
2700	Payable: FOEL Advance		2,308,080.64
2701	2701: A/R: VPPRP VPK Provider Advance	3,811.04	
2710	Payable: Interest		1,655.20

Early Learning Coalition of Marion County, Inc.

Normal Trial Balance - TB ZH

From 7/1/2026 Through 7/31/2026

Account Code	Account Title	Debit Balance	Credit Balance
2720	Payable: Fraud Collections		24,321.93
2900	Deferred Revenue		52,960.24
3000	Net Assets		319,381.34
4001	Grants: State & Federal		1,788,009.93
4100	Revenue: Interest		364.63
4210	Revenue: Provider Trainings		280.00
4905	Revenue: Facility Rental	0.00	
4991	Realized Gain on Investments		14,810.87
4992	Unrealized Gain on Investments	16,034.44	
4999	In-kind		1,069.32
5000	Salary: Directors (990 reportable)	14,423.11	
5001	Salary: Exempt (Other)	139,325.11	
5002	Salary: Hourly	98,283.92	
5005	Payroll Tax: Social Security	15,089.03	
5006	Payroll Tax: Medicare	3,528.86	
5007	Payroll Tax: SUTA	5.57	
5010	Insurance: Health	22,400.00	
5011	Insurance: Dental	1,103.70	
5020	Retirement: ER Contribution	9,233.51	
5030	Insurance: Life	391.88	
5031	Insurance: Short-term Disability	954.34	
5100	Staff Development	325.00	
6002	Professional Services: Auditing	3,500.00	
6005	Professional Services: IT management	6,090.00	
6010	Professional Services: Legal	544.00	
6030	Professional Services: Repairs & Maintenance	305.76	
6035	Professional Services: Other	0.00	
6040	Prof Service: Payroll	1,458.00	
6500	Direct Services: Child Care	1,393,078.59	
6501	Direct Services - Prior Year	36,886.22	
7001	Utilities	2,415.41	
7005	Janitorial Services	2,581.00	
7007	Lawn Service	300.00	
7008	Security System	432.32	
7009	Pest Control	170.00	
7050	Postage, Freight, and Delivery	80.34	
7150	Office Supplies and Expenses	37.18	
7151	Printing: Copier	891.79	
7200	Communications: Land Line	1,154.10	
7201	Communications: Cellular	230.84	
7202	Communications: Internet	137.97	
7251	Insurance and Surety Bonds: D&O	10,980.72	
7255	Insurance and Surety Bonds: Automobile	2,050.00	
7260	Insurance and Surety Bonds: General Liability	284.82	
7270	Insurance and Surety Bonds: Property	25,638.73	
7275	Insurance and Surety Bonds: Other	6,308.48	
7401	Quality and Classroom Material	640.00	
7420	Scholarships and Other Education Opportunities	1,575.00	
7501	Travel: In-State	1,686.30	
7600	Admin Fees (Comm Fdt)	161.50	
7601	Bank Fees	482.65	
7602	Merchant Service Fees	12.46	

Early Learning Coalition of Marion County, Inc.

Normal Trial Balance - TB ZH

From 7/1/2026 Through 7/31/2026

Account Code	Account Title	Debit Balance	Credit Balance
7605	Software-Licenses-Support	8,595.29	
7610	Web service, hosting, support, back-up services & Maintenanc	270.00	
7615	Other employee related expenditures	14.00	
7620	Membership Dues	6,325.00	
7625	Taxes, licenses and fees	15.77	
7901	Vending Machine Supplies	330.95	
8535	Books	10,740.89	
9001	Depreciation	2,223.15	
9999	In-kind Expenditure	1,069.32	
Report Total		6,669,080.53	6,669,080.53
Report Difference		0.00	

ELC OF MARION COUNTY EXECUTIVE SUMMARY

Version: 26.7.1.1

TARGETS AND RESTRICTIONS

SR Direct Services Min: 78%	1,280,466 + 1,757,931	72.8%
SR Admin Max: 5%	74,389 + 1,757,931	4.232%
SR Admin/NonDirect/Quality Max: 22%	477,465 + 1,757,931	27.2%
SR Quality Min: 4%	182,359 + 1,757,931	10.4%
SR Match Max: \$143,860		0.00
Dollar-for-Dollar Match:		0.00
VPK Admin Max: 5%	13,188 43,869	30.063%
SR Plus Admin Max: 5%		0.0%

PROGRAM TOTALS

SR Total
 SR Admin
 SR Non-Direct
 SR Quality
 SR Direct Services*
 Quality Performance
 QPI Shortfall
 SR Match
 Special Needs
 Spec Needs Shortfall
 Gold Seal
 SR Plus
 VPK Total
 VPK Admin
 VPK DS
 VPK PA
 * includes SR Match, Gold S

YTD MATCH SUMMARY

	Cash in EFSM	Cash not in EFSM	Total Cash	Public Funds
<u>Cost Type</u>				
Direct Service	.00	.00	0.00	
Admin	.00	.00	0.00	
All Non Direct	.00	.00	0.00	

ELC of Marion County

Reporting on August 31, 2026 Financial Statements

Fiscal year 2026-2027

Finance Notes:

Tick marks below correspond to the matching tick marks on the attached August 31, 2026 Balance Sheet, Income Statement – All Funds, and the SR and VPK fund-level Income Statements. Income statement amounts are year to date (July 1 – August 31, 2026) compared with the same two months last year. All variances over \$10,000 are explained.

Balance Sheet:

- **(a)** All cash accounts (Operating, Unrestricted, Building, PayPal, Community Foundation, and petty cash) have been reconciled as of August 31, 2026. We are holding approximately \$1,905,000 in cash, up about \$518,000 from July as FOEL reimbursements for prior months came in. Cash naturally fluctuates with the timing of the FOEL reimbursement draw cycle — balances dip as expenditures are paid out and build back up as reimbursement is received.
- **(b)** Accounts receivable is approximately \$1,911,000, of which approximately \$1,796,000 is due from FOEL (down from \$2,285,000 in July as DEL paid outstanding invoices). Receivables from other grants increased to approximately \$90,000. See AR Aging Schedule.
- **(c)** We have fixed assets with a net book value of approximately \$517,000 (shown as “Other” on the balance sheet). The decrease from July is the \$2,223 monthly depreciation.
- **(d)** Accounts payable is approximately \$1,415,000 (net of the A/P conversion adjustment) and is current.
- **(e)** Due to DEL (Payable: FOEL Advance) is approximately \$2,308,000, unchanged from July.
- **(f)** Total Net Assets is approximately \$371,000.

Income Statement – All Funds

- **(1)** Grant Revenue increased year over year, from \$3,068,860 to \$3,490,574 (+\$421,714, +13.7%). Because our grants are cost-reimbursement, revenue rises with spending. The increase is in SR (+\$367,498) and VPK (+\$73,648), driven by serving more children (see 6 and 11). Revenue from other grants is down \$19,432.
- **(2)** Salaries (Personnel Expenses) increased year over year, from \$434,380 to \$511,896 (+\$77,516, +17.8%). The increase comes from July, which had 3 payroll cycles this year. August on its own was \$207,157, about \$20,700 lower than August 2025 (\$227,905).
- **(3)** Program Expenses increased year over year, from \$2,505,604 to \$2,868,047 (+\$362,443, +14.5%), driven by higher SR enrollment (+\$314,085, see 8) and VPK (+\$65,918, see 12).
- **(4)** Maintenance & Repairs decreased year over year, from \$42,138 to \$2,926 (-\$39,212), and Miscellaneous increased from \$20,820 to \$63,328 (+\$42,508). Last year general liability insurance was recorded in Maintenance & Repairs; this year all insurance is recorded in Miscellaneous. Taken together, the two lines went from \$62,957 to \$66,253 (+\$3,296), about the same as last year.
- **(5)** Net Revenue Over Expenditures is a deficit of \$8,888, compared with a surplus of \$22,568 last year (-\$31,455). SR (+\$3,729) and VPK (\$0) are essentially break-even as cost-reimbursement grants, so the deficit sits in our other funds (about \$12,600).
- **(6)** (see SR Income Statement) SR Grant Revenue increased year over year, from \$2,722,815 to \$3,090,313 (+\$367,498, +13.5%), in line with higher SR spending.
- **(7)** SR Personnel Expenses show a decrease, from \$489,342 to \$458,454 (-\$30,888), but the prior-year amount is not a fair comparison. Last year, SR and VPK personnel together (\$520,758) came to more than total agency personnel for the same two months (\$434,380), which reflects how prior-year costs were allocated between funds. Total agency personnel is up, as explained in (2).

- **(8)** SR Program Expenses increased year over year, from \$2,179,530 to \$2,493,615 (+\$314,085, +14.4%). We served 2,347 children in July and 2,228 in August, compared with 2,048 and 2,112 last year — 4,575 child-months versus 4,160 (+10.0%). The average cost per child per month went from about \$524 to \$545 (+4.0%). About \$217,000 of the increase comes from serving more children and about \$97,000 from the higher cost per child.
- **(9)** SR Maintenance & Repairs decreased \$25,611 and Miscellaneous increased \$71,232 because of the same insurance classification change described in (4).
- **(10)** SR Net Revenue Over Expenditures is a surplus of \$3,729, compared with a deficit of \$28,484 last year (+\$32,213). SR is cost-reimbursed and should net close to zero; the small difference is timing of revenue recognition.
- **(11)** (see VPK Income Statement) VPK Grant Revenue increased year over year, from \$314,804 to \$388,452 (+\$73,648, +23.4%), in line with higher VPK spending. VPK nets to \$0 for the year to date.
- **(12)** VPK Program Expenses (direct services) increased year over year, from \$269,189 to \$335,107 (+\$65,918, +24.5%), due to serving more VPK children as the 2026-27 school year began in August. As always, we serve all children who are four years old and want to attend, regardless of funding.
- **(13)** VPK Maintenance & Repairs decreased \$11,141 and Miscellaneous increased \$13,436 because of the same insurance classification change described in (4).

Dashboard mandates:

SR Admin = 4.05% (under the 5% maximum)

SR Direct Services = 79.2% (meets the 78% minimum; up from 72.8% in July)

SR Admin/Non-Direct/Quality = 20.8% (under the 22% maximum)

Quality = 9.0% (above the 4% minimum)

VPK Admin = 15.62% (over the 5% maximum). This is expected early in the year. VPK provider payments are only \$308,600 so far because the school year started in August, while admin costs run evenly all year. The 5% cap applies to the full fiscal year, and the percentage will drop as provider payments ramp up.

Early Learning Coalition of Marion County, Inc.

Balance Sheet

As of 8/31/2026

(In Whole Numbers)

<u>Current Year</u>		
Assets		
Cash: Operating (0332)	1,614,214	A
Cash: Unrestricted (0340)	130,099	
Cash: Building (0464)	30,302	
Cash: PayPal	317	
Cash: Community Foundation	130,395	
Petty Cash: Vending Machine	71	B
A/R: FOEL	1,796,267	
A/R: Other Grants	89,742	
A/R: Overpayments	1,061	
A/R: Clearing	23,433	
Prepaid: Postage	1,058	C
Prepaid: Other	14,487	
Prepaid: Travel Advance	3,546	
Other	517,415	
Total Assets	4,352,406	
Liabilities		
Credit Card (South State - VISA)	9,580	D
Accounts Payable	1,441,085	
A/P: Conversion	(25,986)	
Payable: Accrued PLT	151,721	
Payable: Medicare	(0)	
Payable: SUTA	(36)	E
Payable: Health Insurance	(14,440)	
Payable: Dental Insurance	(231)	
Payable: Vision Insurance	1,927	
Payable: ER - 403(b)	(2,068)	
Payable: EE - 403(b)	11,742	F
Payable: EE - Roth IRA	1,697	
Payable: Life Insurance	137	
Payable: Short-term Disability	255	
Payable: Long-term Disability	(973)	
Payable: AFLAC	1,831	F
Payable: Colonial Life	(296)	
Payable: United Way Deductions	10,933	
Payable: Wage Garnishment	(264)	
Payable: Workers Compensation	(7,145)	
Payable: FOEL Advance	2,308,081	
2701: A/R: VPPRP VPK Provider Advance	30,380	
Payable: Interest	1,724	
Payable: Fraud Collections	24,322	
Deferred Revenue	37,139	
Total Liabilities	3,981,117	
Net Assets	371,289	
Total Liabilities and Net Assets	4,352,406	

Early Learning Coalition of Marion County, Inc.

Aged Receivables by Invoice Date
Aging Date - 8/31/2026
From 7/1/2026 Through 8/31/2026

Customer ID	Customer Name	Invoice Date	Invoice Number	Description	Total	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due
Children's Forum	Children's Forum , Inc - HMG	7/20/2026	25hmgfa-12812	JUNE HMG INV	28,736.10	0.00	0.00	28,736.10	0.00	0.00
Children's Forum		8/21/2026	26HMGFA-12R31	JUL HMG INV	11,808.29	0.00	11,808.29	0.00	0.00	0.00
Total Children's Forum	Children's Forum , Inc - HMG				40,544.39	0.00	11,808.29	28,736.10	0.00	0.00
FOEL	Florida's Office of Early Learning	8/30/2026	3260626R2	DEL JUN 2026 2ND INV	26,506.81	0.00	26,506.81	0.00	0.00	0.00
FOEL		9/15/2026	3270826P1	AUG PYM ADJ 1ST	10,457.18	10,457.18	0.00	0.00	0.00	0.00
FOEL		9/23/2026	3270826R1	DEL AUG 2026 INV	1,718,758.60	1,718,758.60	0.00	0.00	0.00	0.00
Total FOEL	Florida's Office of Early Learning				1,755,722.59	1,729,215.78	26,506.81	0.00	0.00	0.00
Joan S. Hatten	Joan S. Hatten	6/30/2021	FY19SR-J.S.Hatten	Joan S. Hatten 2018 - 2019 - Overpayment SR Recon	1,061.26	0.00	0.00	0.00	0.00	1,061.26
Total Joan S. Hatten	Joan S. Hatten				1,061.26	0.00	0.00	0.00	0.00	1,061.26
MCBOCC	Marion County Board of County Commissioners	9/30/2022	082022MCMA	MCBOCC - Match - September 2022	(39.96)	0.00	0.00	0.00	0.00	(39.96)
MCBOCC		6/30/2024	062024MCMA	MCBOCC- MATCH- June 2024	0.03	0.00	0.00	0.00	0.00	0.03
MCBOCC		1/31/2025	0125DPL	DPIL Early Literacy Assistance FY24-25	2,349.79	0.00	0.00	0.00	0.00	2,349.79
MCBOCC		2/27/2026	0126DPL	DPIL ELA Assistance FY 26 - Jan 2026	(0.03)	0.00	0.00	0.00	0.00	(0.03)
MCBOCC		6/1/2026	0126DPL-b	DPIL ELA Assistance FY26 JAN INV Adj	0.03	0.00	0.00	0.00	0.00	0.03

Early Learning Coalition of Marion County, Inc.

Aged Receivables by Invoice Date
Aging Date - 8/31/2026
From 7/1/2026 Through 8/31/2026

Customer ID	Customer Name	Invoice Date	Invoice Number	Description	Total	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due
MCBOCC		6/30/2026	0526DPL	DPIL ELA ASSISTANCE FY26 MAY INV	513.22	0.00	0.00	0.00	513.22	0.00
MCBOCC		6/30/2026	0626MCMA	MATCH JUNE 2026 INV	72,604.41	0.00	0.00	0.00	72,604.41	0.00
Total MCBOCC	Marion County Board of County Commissioners				75,427.49	0.00	0.00	0.00	73,117.63	2,309.86
SBMC	The School Board of Marion County, Florida	12/18/2025	YPP-1125	YPP Invoices	1,780.37	0.00	0.00	0.00	0.00	1,780.37
SBMC		5/19/2026	YPP-0126b	YPP RECONCILIATIO... INVOICES 25-26	1,477.67	0.00	0.00	0.00	0.00	1,477.67
SBMC		5/19/2026	ypp-0925b	YPP RECONCILIATIO... INVOICES 25-26	165.92	0.00	0.00	0.00	0.00	165.92
SBMC		5/19/2026	YPP-1125b	YPP RECONCILIATIO... INVOICES 25-26	191.22	0.00	0.00	0.00	0.00	191.22
SBMC		5/19/2026	YPP-1225b	YPP RECONCILIATIO... INVOICES 25-26	1,045.25	0.00	0.00	0.00	0.00	1,045.25
SBMC		5/21/2026	YPP-0825b	YPP RECONCILIATIO... INVOICES 25-26	163.30	0.00	0.00	0.00	0.00	163.30
SBMC		6/29/2026	YPP-0526	YPP-0526	3,395.53	0.00	0.00	0.00	3,395.53	0.00
SBMC		6/30/2026	YPP-0426-Adj	APR 2026 YPP INV ADJ	3,395.53	0.00	0.00	0.00	3,395.53	0.00
SBMC		6/30/2026	YPP-1025-b	YPP Oct 2025 Adjustment	2,699.67	0.00	0.00	0.00	2,699.67	0.00
Total SBMC	The School Board of Marion County, Florida				14,314.46	0.00	0.00	0.00	9,490.73	4,823.73
UWMC	United Way of Marion County, Inc.	6/1/2026	202606-UW	United Way Invoice - JUN 2026	(0.01)	0.00	0.00	0.00	0.00	(0.01)

Early Learning Coalition of Marion County, Inc.

Aged Receivables by Invoice Date
Aging Date - 8/31/2026
From 7/1/2026 Through 8/31/2026

Customer ID	Customer Name	Invoice Date	Invoice Number	Description	Total	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due
Total UWMC	United Way of Marion County, Inc.				(0.01)	0.00	0.00	0.00	0.00	(0.01)
Report Total					1,887,070.18	1,729,215.78	38,315.10	28,736.10	82,608.36	8,194.84

Early Learning Coalition of Marion County, Inc.
Aged Payables by Due Date - Zh AP Aging Report - All Funds
Aging Date - 8/31/2026
From 7/1/2026 Through 8/31/2026

Vendor Name	Invoice Number	Invoice/Cre... Date	Due Date	Current	1 - 30 Days Past Due	31 - 60 Days Past Due	61 - 90 Days Past Due	Over 90 Days Past Due	Total
Turf Surfers LawnScape, LLC	TS-082026	8/1/2026	8/1/2026	0.00	300.00	0.00	0.00	0.00	300.00
Total Turf Surfers LawnScape, LLC				0.00	300.00	0.00	0.00	0.00	300.00
Verizon Wireless	913502808-00004-01	5/30/2023	6/8/2023	0.00	0.00	0.00	0.00	(968.28)	(968.28)
Total Verizon Wireless				0.00	0.00	0.00	0.00	(968.28)	(968.28)
Walmart	V-012023-C	2/2/2023	2/2/2023	0.00	0.00	0.00	0.00	15.00	15.00
Total Walmart				0.00	0.00	0.00	0.00	15.00	15.00
Wendy Williams	TR072026-11	7/24/2026	8/23/2026	0.00	52.56	0.00	0.00	0.00	52.56
Total Wendy Williams				0.00	52.56	0.00	0.00	0.00	52.56
West Family Learning Center East, LLC	0726-SP02-6656-000	8/31/2026	9/21/2026	693.44	0.00	0.00	0.00	0.00	693.44
	SR0826-811326656-...	8/31/2026	9/21/2026	12,178.73	0.00	0.00	0.00	0.00	12,178.73
Total West Family Learning Center East, LLC				12,872.17	0.00	0.00	0.00	0.00	12,872.17
Wilma Martin Family Daycare Home	0626-SY02-8920-000	8/31/2026	9/21/2026	(491.60)	0.00	0.00	0.00	0.00	(491.60)
	0726-SP02-8920-000	8/31/2026	9/21/2026	(228.94)	0.00	0.00	0.00	0.00	(228.94)
	SR0826-882898920-...	8/31/2026	9/21/2026	9,909.92	0.00	0.00	0.00	0.00	9,909.92
Total Wilma Martin Family Daycare Home				9,189.38	0.00	0.00	0.00	0.00	9,189.38
Wilson's Lovable Daycare, LLC	SR0826-825414548-...	8/31/2026	9/21/2026	8,143.32	0.00	0.00	0.00	0.00	8,143.32
Total Wilson's Lovable Daycare, LLC				8,143.32	0.00	0.00	0.00	0.00	8,143.32
Wiz Kids Learning Academy	SR0826-472528160-...	8/31/2026	9/21/2026	17,788.57	0.00	0.00	0.00	0.00	17,788.57
Total Wiz Kids Learning Academy				17,788.57	0.00	0.00	0.00	0.00	17,788.57
Report Total				1,439,963.91	8,927.03	5,589.80	3,028.63	(7,807.47)	1,449,701.90

Early Learning Coalition of Marion County, Inc.

Statement of Revenues and Expenditures - Detail

From 7/1/2026 Through 8/31/2026

	Current Period Actual	Prior Year Current Period Actual	Current Period Change	Current Year % Change	
Operating Revenue					
Grant Revenue	3,490,573.64	3,068,859.93	421,713.71	13.74	1
Contributions	2,368.77	4,758.69	(2,389.92)	(50.22)	
Program Revenue	560.00	202.00	358.00	177.23	
Investment Income	552.90	423.17	129.73	30.66	
Other Income	216.67	866.68	(650.01)	(75.00)	
Total Operating Revenue	<u>3,494,271.98</u>	<u>3,075,110.47</u>	<u>419,161.51</u>	<u>13.63</u>	
Total Revenue	<u>3,494,271.98</u>	<u>3,075,110.47</u>	<u>419,161.51</u>	<u>13.63</u>	
Expenditures					
Personnel Expenses	511,895.80	434,379.67	77,516.13	17.85	2
Program Expenses	2,868,047.00	2,505,603.54	362,443.46	14.47	3
Professional Fees	23,281.76	15,694.72	7,587.04	48.34	
Supplies	1,045.54	2,576.82	(1,531.28)	(59.43)	
Telephone	3,024.32	4,312.30	(1,287.98)	(29.87)	
Postage & Shipping	167.97	66.90	101.07	151.08	
Occupancy	14,015.53	11,944.35	2,071.18	17.34	
Maintenance & Repairs	2,925.58	42,137.80	(39,212.22)	(93.06)	4
Equipment Rental	270.12	270.12	0.00	0.00	
Conferences, Conventions & Meetings	2,705.25	750.00	1,955.25	260.70	
Printing & Publications	1,381.77	3,440.47	(2,058.70)	(59.84)	
Dues & Subscriptions	6,625.00	6,100.00	525.00	8.61	
Depreciation	4,446.30	4,446.30	0.00	0.00	
Miscellaneous	63,327.54	20,819.50	42,508.04	204.17	4
Total Expenditures	<u>3,503,159.48</u>	<u>3,052,542.49</u>	<u>450,616.99</u>	<u>14.76</u>	
Net Revenue Over Expenditures	<u>(8,887.50)</u>	<u>22,567.98</u>	<u>(31,455.48)</u>	<u>(139.38)</u>	5

Early Learning Coalition of Marion County, Inc.

Statement of Revenues and Expenditures - Detail

From 7/1/2026 Through 8/31/2026

	Current Period Actual	Prior Year Current Period Actual	Current Period Change	Current Year % Change	
Operating Revenue					
Grant Revenue	<u>3,090,312.86</u>	<u>2,722,814.77</u>	<u>367,498.09</u>	<u>13.50</u>	6
Total Operating Revenue	<u>3,090,312.86</u>	<u>2,722,814.77</u>	<u>367,498.09</u>	<u>13.50</u>	
Total Revenue	<u>3,090,312.86</u>	<u>2,722,814.77</u>	<u>367,498.09</u>	<u>13.50</u>	
Expenditures					
Personnel Expenses	458,453.53	489,341.81	(30,888.28)	(6.31)	7
Program Expenses	2,493,614.97	2,179,530.13	314,084.84	14.41	8
Professional Fees	16,615.97	14,310.24	2,305.73	16.11	
Supplies	878.95	947.90	(68.95)	(7.27)	
Telephone	2,790.73	3,540.93	(750.20)	(21.19)	
Postage & Shipping	158.65	41.97	116.68	278.01	
Occupancy	12,745.72	8,613.46	4,132.26	47.97	
Maintenance & Repairs	3,797.49	29,408.96	(25,611.47)	(87.09)	9
Equipment Rental	235.30	0.00	235.30	100.00	
Conferences, Conventions & Meetings	2,680.25	750.00	1,930.25	257.37	
Printing & Publications	1,295.33	3,280.85	(1,985.52)	(60.52)	
Dues & Subscriptions	6,550.00	6,025.00	525.00	8.71	
Depreciation	514.35	486.97	27.38	5.62	
Miscellaneous	<u>86,252.55</u>	<u>15,020.25</u>	<u>71,232.30</u>	<u>474.24</u>	9
Total Expenditures	<u>3,086,583.79</u>	<u>2,751,298.47</u>	<u>335,285.32</u>	<u>12.19</u>	
Net Revenue Over Expenditures	<u>3,729.07</u>	<u>(28,483.70)</u>	<u>32,212.77</u>	<u>(113.09)</u>	10

Early Learning Coalition of Marion County, Inc.

Statement of Revenues and Expenditures - Detail

From 7/1/2026 Through 8/31/2026

	Current Period Actual	Prior Year Current Period Actual	Current Period Change	Current Year % Change	
Operating Revenue					
Grant Revenue	388,452.49	314,804.41	73,648.08	23.39	11
Total Operating Revenue	388,452.49	314,804.41	73,648.08	23.39	
Total Revenue	388,452.49	314,804.41	73,648.08	23.39	
Expenditures					
Personnel Expenses	32,055.25	31,415.78	639.47	2.04	
Program Expenses	335,107.18	269,188.75	65,918.43	24.49	12
Professional Fees	2,530.71	1,384.48	1,146.23	82.79	
Supplies	125.28	120.75	4.53	3.75	
Telephone	233.59	666.37	(432.78)	(64.95)	
Postage & Shipping	8.25	1.91	6.34	331.94	
Occupancy	1,269.81	979.42	290.39	29.65	
Maintenance & Repairs	1,462.91	12,603.84	(11,140.93)	(88.39)	13
Equipment Rental	34.82	0.00	34.82	100.00	
Printing & Publications	86.44	81.67	4.77	5.84	
Depreciation	99.73	127.11	(27.38)	(21.54)	
Miscellaneous	15,438.52	2,002.69	13,435.83	670.89	13
Total Expenditures	388,452.49	318,572.77	69,879.72	21.94	
Net Revenue Over Expenditures	0.00	(3,768.36)	3,768.36	(100.00)	

Early Learning Coalition of Marion County, Inc.
Normal Trial Balance - Board Report - Unposted Transactions Included In Report
From 7/1/2026 Through 8/31/2026

Account Code	Account Title	Debit Balance	Credit Balance
1000	Cash: Operating (0332)	1,614,213.66	
1010	Cash: Unrestricted (0340)	130,099.24	
1020	Cash: Building (0464)	30,302.48	
1050	Cash: PayPal	316.54	
1080	Cash: Community Foundation	130,394.70	
1091	Petty Cash: Vending Machine	70.74	
1098	Credit Card (South State - VISA)		1,055.93
1200	A/R: FOEL	1,796,266.98	
1210	A/R: Other Grants	89,741.94	
1220	A/R: Overpayments	1,061.26	
1299	A/R: Clearing	23,432.88	
1400	Prepaid: Postage	1,057.58	
1401	Prepaid: Insurance		45,262.75
1403	Prepaid: Other	14,486.74	
1405	Prepaid: Travel Advance	3,545.64	
1500	Fixed Assets: Equipment	58,707.26	
1501	Fixed Assets: Furniture	5,300.00	
1502	Fixed Assets: Building	856,517.59	
1503	Fixed Assets: Land	116,960.14	
1600	Accumulated Depreciation: Equipment		58,707.10
1601	Accumulated Depreciation: Furniture		5,300.00
1602	Accumulated Depreciation: Building		456,062.77
2000	Accounts Payable		1,449,701.90
2099	A/P: Conversion	25,985.97	
2203	Payable: Accrued PLT		151,720.97
2206	Payable: Medicare	0.39	
2207	Payable: SUTA	35.68	
2210	Payable: Health Insurance	14,440.25	
2211	Payable: Dental Insurance	231.07	
2212	Payable: Vision Insurance		1,927.43
2220	Payable: ER - 403(b)	2,068.06	
2221	Payable: EE - 403(b)		11,741.92
2222	Payable: EE - Roth IRA		1,697.44
2230	Payable: Life Insurance		137.39
2231	Payable: Short-term Disability		254.86
2232	Payable: Long-term Disability	972.67	
2240	Payable: AFLAC		1,830.88
2245	Payable: Colonial Life	295.88	
2250	Payable: United Way Deductions		10,933.40
2255	Payable: Wage Garnishment	263.92	
2265	Payable: Workers Compensation	7,144.78	
2700	Payable: FOEL Advance		2,308,080.64
2701	2701: A/R: VPPRP VPK Provider Advance		30,380.32
2710	Payable: Interest		1,723.73
2720	Payable: Fraud Collections		24,321.93
2900	Deferred Revenue		37,139.48
3000	Net Assets		379,315.04
4001	Grants: State & Federal		3,490,573.64
4100	Revenue: Interest		552.90
4210	Revenue: Provider Trainings		560.00
4905	Revenue: Facility Rental		216.67
4991	Realized Gain on Investments		14,849.18
4992	Unrealized Gain on Investments	14,080.77	
4999	In-kind		2,368.77
5000	Salary: Directors (990 reportable)	24,528.88	

Early Learning Coalition of Marion County, Inc.
Normal Trial Balance - Board Report - Unposted Transactions Included In Report
From 7/1/2026 Through 8/31/2026

Account Code	Account Title	Debit Balance	Credit Balance
5001	Salary: Exempt (Other)	233,148.13	
5002	Salary: Hourly	162,963.91	
5005	Payroll Tax: Social Security	25,094.17	
5006	Payroll Tax: Medicare	5,868.78	
5007	Payroll Tax: SUTA	5.57	
5010	Insurance: Health	39,886.58	
5011	Insurance: Dental	2,207.40	
5020	Retirement: ER Contribution	15,496.98	
5030	Insurance: Life	783.76	
5031	Insurance: Short-term Disability	1,911.64	
5100	Staff Development	2,705.25	
6002	Professional Services: Auditing	3,500.00	
6005	Professional Services: IT management	9,635.00	
6010	Professional Services: Legal	5,071.32	
6030	Professional Services: Repairs & Maintenance	590.76	
6035	Professional Services: Other	2,000.00	
6040	Prof Service: Payroll	2,881.44	
6500	Direct Services: Child Care	2,805,276.28	
6501	Direct Services - Prior Year	37,333.92	
7001	Utilities	4,931.76	
7005	Janitorial Services	5,162.00	
7006	Janitorial Supplies	345.00	
7007	Lawn Service	600.00	
7008	Security System	1,018.51	
7009	Pest Control	1,958.26	
7050	Postage, Freight, and Delivery	167.97	
7100	Equipment Lease and Maintenance	270.12	
7150	Office Supplies and Expenses	1,045.54	
7151	Printing: Copier	1,381.77	
7200	Communications: Land Line	2,286.35	
7201	Communications: Cellular	461.84	
7202	Communications: Internet	276.13	
7251	Insurance and Surety Bonds: D&O	21,961.44	
7255	Insurance and Surety Bonds: Automobile	4,100.00	
7260	Insurance and Surety Bonds: General Liability	569.64	
7270	Insurance and Surety Bonds: Property	51,277.46	
7275	Insurance and Surety Bonds: Other	13,686.53	
7401	Quality and Classroom Material	640.00	
7410	Consumer Education and Outreach Material	117.57	
7420	Scholarships and Other Education Opportunities	3,125.00	
7501	Travel: In-State	2,099.39	
7510	Travel: In Service Area	294.52	
7600	Admin Fees (Comm Fdt)	321.71	
7601	Bank Fees	894.36	
7602	Merchant Service Fees	24.92	
7604	Finance Charges	184.72	
7605	Software-Licenses-Support	10,914.55	
7610	Web service, hosting, support, back-up services & Maintenanc	270.00	
7615	Other employee related expenditures	14.00	
7616	Backgroud Screening	194.00	

Early Learning Coalition of Marion County, Inc.
Normal Trial Balance - Board Report - Unposted Transactions Included In Report
From 7/1/2026 Through 8/31/2026

Account Code	Account Title	Debit Balance	Credit Balance
7620	Membership Dues	6,625.00	
7625	Taxes, licenses and fees	1,612.15	
7901	Vending Machine Supplies	330.95	
8535	Books	21,283.35	
8550	Food services (Unallowable)	270.88	
9001	Depreciation	4,446.30	
9999	In-kind Expenditure	2,368.77	
Report Total		8,486,417.04	8,486,417.04
Report Difference			0.00

ELC OF MARION COUNTY EXECUTIVE SUMMARY

Version: 26.7.1.1

TARGETS AND RESTRICTIONS

SR Direct Services Min: 78%	2,339,886 + 37,396 2,999,865	79.2%
SR Admin Max: 5%	121,568 + 2,999,865	4.052%
SR Admin/NonDirect/Quality Max: 22%	622,583 + 2,999,865	20.8%
SR Quality Min: 4%	271,182 + 2,999,865	9.0%
SR Match Max: \$143,860		769.61
Dollar-for-Dollar Match:		769.61
VPK Admin Max: 5%	48,209 308,600	15.622%
SR Plus Admin Max: 5%		0.9%

PROGRAM TOTALS

SR Total
 SR Admin
 SR Non-Direct
 SR Quality
 SR Direct Services*
 Quality Performance
 QPI Shortfall
 SR Match
 Special Needs
 Spec Needs Shortfall
 Gold Seal
 SR Plus
 VPK Total
 VPK Admin
 VPK DS
 VPK PA

* includes SR Match, Gold Seal

YTD MATCH SUMMARY

Cost Type	Cash in EFSM	Cash not in EFSM	Total Cash	Public Funds
Direct Service	37,396.48	.00	37,396.48	
Admin	.00	.00	0.00	
All Non Direct	.00	.00	0.00	



Early Learning Coalition of Marion County

Action Sheet

FULL COALITION BOARD

October 22, 2026

SUBJECT: Revised Fiscal Policy: Section – Cash Management

Fiscal Impact: N/A

PROPOSED ACTION

Make a recommendation to approve the proposed revisions to FA130 – Cash Management Policy to ensure compliance with current program guidance and federal regulations issued by the Division of Early Learning.

BACKGROUND INFORMATION

The current Fiscal Manual contains both policies and detailed procedures within the Board-approved document. This can require Board action when a procedure needs to be updated even though the underlying policy has not changed.

At the recommendation of the Executive Committee, staff began reviewing the Coalition's Fiscal Manual by section to ensure that the manual remains current, effective, and aligned with the Coalition's operations and applicable requirements.

The review is intended to:

- Remove outdated or duplicative language;
- Ensure policies continue to reflect appropriate internal controls;
- Align fiscal requirements with current federal, state, DEL, grant, and contractual requirements;
- Ensure consistency among the various fiscal sections;
- Clearly distinguish Board-level policy from management-level procedures; and
- Create a more efficient process for maintaining and updating the Fiscal Manual.

FA130 – Cash Management is the first section being presented through this revised process.

On September 10, 2026, the Executive Committee approved the revised Fiscal Policy: Section – Cash Management as stated above.

Supporting Documentation Included:

- 2026 – 2027 ELCMC Fiscal Policy: Section 130 Cash Management

Supporting Documentation Available:

- Draft Procedures FA130.01 – FA130.08
- 2018 Fiscal Manual



Early Learning
Coalition OF Marion
County

9/10/2026

Administrative / Fiscal Policy Manual

LaTrisha Sims, Chief Executive Officer

Board approved TBD

Effective TBD

FA100 – Financial Governance and Internal Controls
FA100.01 Purpose and Scope of the Fiscal Policy Manual
FA100.02 Financial Management Principles
FA100.03 Roles and Responsibilities
FA100.04 Internal Controls
FA100.05 Segregation of Duties
FA100.06 Fraud, Waste, and Abuse Prevention

FA110 – Budgeting and Financial Planning
FA110.01 Annual Budget Development
FA110.02 Budget Review and Approval
FA110.03 Budget Monitoring
FA110.04 Budget Amendments

FA120 – Accounting and Financial Reporting
FA120.01 Accounting Standards and Principles
FA120.02 Chart of Accounts
FA120.03 Financial Records Management
FA120.04 Financial Reporting

FA130 – Cash Management

The Coalition shall maintain a comprehensive cash management system that ensures all funds are received, safeguarded, deposited, disbursed, reconciled, and reported in accordance with Generally Accepted Accounting Principles (GAAP), 2 CFR Part 200, Division of Early Learning (DEL) Program Guidance 240.01, applicable grant and contract requirements, applicable federal and state laws and regulations, and the Coalition's Internal Control Framework.

The Coalition shall manage cash and federal and other restricted funds in a manner that maintains sufficient liquidity to meet authorized financial obligations while minimizing the time between the receipt or transfer of funds and their disbursement for allowable expenditures.

The Coalition shall establish, document, maintain, and monitor internal controls designed to protect assets, prevent and detect fraud, waste, abuse, and misuse of funds, ensure financial accountability, maintain accurate financial records, support timely and reliable financial reporting, and comply with applicable grant and regulatory requirements.

Cash management controls shall include segregation of duties, documented approvals, management oversight, safeguarding of assets, monitoring activities, reconciliations, appropriate access controls, and retention of records sufficient to support audits, monitoring reviews, and financial reporting requirements.

The Coalition shall promptly identify, investigate, correct, and document cash management deficiencies and instances of noncompliance.

FA130.01 Cash Accounts

Reference Procedure: FA26.130.01 V1.0

The Coalition shall establish, maintain, and administer cash and bank accounts in a manner that safeguards Coalition funds, maintains appropriate segregation of funds, and complies with

applicable federal and state laws and regulations, grant and contract requirements, DEL requirements, and Coalition policies.

All Coalition bank accounts shall be established and maintained only for authorized Coalition purposes and shall be subject to appropriate management authorization and oversight.

Coalition funds shall be properly classified, safeguarded, recorded, and administered in accordance with applicable restrictions and requirements. Restricted, grant, and other designated funds shall be accounted for in a manner that permits the Coalition to identify the source and application of funds.

The Coalition shall maintain effective custodial accountability and physical and administrative safeguards over all bank accounts and cash on hand.

Access to bank accounts, online banking systems, payment platforms, and related financial systems shall be limited to authorized personnel based on job responsibilities. Access shall be periodically reviewed and promptly removed when no longer required.

Interest and other earnings on Coalition funds shall be identified, recorded, monitored, and accounted for in accordance with applicable federal and state requirements, DEL requirements, grant and contract agreements, and applicable funding restrictions.

FA130.02 Cash Receipts

Reference Procedure: FA26.130.02 V1.0

The Coalition shall maintain effective internal controls over the receipt, documentation, safeguarding, depositing, and recording of all funds received from authorized sources.

All cash receipts shall be properly identified, supported by adequate documentation, safeguarded, deposited in accordance with FA130.03 – Deposits, and accurately recorded in the Coalition's accounting records.

Cash receipts shall be recorded in a timely manner and in sufficient detail to identify the source, amount, funding source, and applicable accounting classification.

The Coalition shall maintain appropriate segregation of duties among the functions of receiving, safeguarding, recording, depositing, reconciling, and approving financial transactions.

When complete segregation of duties is not practical due to staffing or operational limitations, compensating controls shall be implemented, documented, and periodically reviewed.

FA130.03 Deposits

Reference Procedure: FA26.130.03 V1.0

The Coalition shall ensure that all funds received are deposited intact and in a timely manner into authorized Coalition bank accounts.

Deposits shall be supported by adequate documentation and processed in accordance with sound cash management practices designed to safeguard assets, maintain accurate accounting records, and minimize the risk of loss, theft, or misuse.

Funds shall not be retained outside authorized Coalition-controlled locations or accounts or used for purposes other than those authorized by applicable laws, regulations, funding agreements, and Coalition policies.

Funds awaiting deposit shall be secured in a locked location with restricted access. Access to undeposited funds shall be limited to authorized personnel.

Deposit records shall be reconciled to supporting receipt documentation and accounting records to ensure completeness and accuracy.

The procedures shall establish the required deposit frequency and any applicable exceptions based on the nature and amount of funds received.

FA130.04 Bank Reconciliations

Reference Procedure: FA26.130.04 V1.0

The Coalition shall reconcile all bank accounts on a monthly basis to ensure the accuracy, completeness, and reliability of financial records.

Bank reconciliations shall be completed timely after the end of each month and shall be prepared by qualified personnel who are independent, to the extent practicable, of cash receipt, disbursement, and bank transaction processing functions.

Completed reconciliations shall be reviewed and approved by management or another designated reviewer who is independent of the preparer.

Reconciling items, unusual transactions, outstanding checks, deposits in transit, electronic transactions, and other discrepancies shall be investigated and resolved promptly.

The Coalition shall monitor outstanding reconciling items and take appropriate corrective action when items remain unresolved beyond established timeframes.

Supporting documentation for bank reconciliations shall be maintained in accordance with applicable record retention requirements.

Bank reconciliations are a key internal control supporting asset accountability, financial integrity, fraud prevention, accurate financial reporting, and compliance with grant, regulatory, and audit requirements.

FA130.05 Cash Flow Management

Reference Procedure: FA26.130.05 V1.0

The Coalition shall manage cash in a manner that maintains sufficient liquidity to meet authorized financial obligations while minimizing the time between the receipt or transfer of federal and other restricted funds and their disbursement for allowable expenditures.

The Coalition shall maintain written procedures for requesting, receiving, transferring, using, monitoring, and reconciling federal and other restricted funds.

Cash flow management shall be based on reasonable and supportable cash flow projections that consider anticipated receipts, expenditures, payroll, grant funding requirements, contractual obligations, and other authorized financial commitments.

The Coalition shall request, draw, transfer, or otherwise obtain funds only in amounts reasonably necessary to meet immediate or near-term allowable expenditures and shall avoid maintaining excess balances of federal or other restricted funds when prohibited by applicable requirements.

Federal and DEL advances shall be monitored and reconciled in accordance with applicable grant agreements, DEL requirements, and federal requirements. Unexpended or excess advances shall be appropriately adjusted, offset, or returned within the required timeframe.

Cash flow management activities shall be appropriately authorized, documented, monitored, and reconciled.

The Coalition shall maintain documentation sufficient to demonstrate compliance with applicable cash management requirements, including the timing and amount of funds received, expenditures made, balances maintained, and amounts returned or remitted.

FA130.06 Program Income

Reference Procedure: FA26.130.06 V1.0

The Coalition shall identify, record, account for, monitor, and report program income in accordance with applicable federal and state laws and regulations, grant and contract agreements, DEL requirements, and Coalition policies.

Program income shall be identified by funding source and accounted for using the method required by the applicable federal award, grant agreement, DEL requirement, or other funding authority.

Program income shall be recorded in the Coalition's accounting records in sufficient detail to identify its source, amount, applicable funding source, and use.

Program income shall be used and accounted for only as permitted by the applicable funding requirements.

The Coalition shall ensure that program income is used for allowable purposes, appropriately reported and reconciled, and returned or remitted when required.

FA130.07 Electronic Funds Transfer

Reference Procedure: FA26.130.07 V1.0

The Coalition authorizes the use of electronic funds transfers (EFTs) only when the transaction supports an approved business purpose, is permitted by the applicable funding source, and is processed through a Coalition-approved financial institution, banking platform, or payment system.

Access to banking and payment systems shall be based on job responsibilities, formally approved, uniquely assigned, periodically reviewed, and promptly removed when no longer required.

No individual shall control all key phases of an EFT. Requesting, initiating, verifying banking information, approving, releasing, recording, reconciling, and reviewing EFTs shall be segregated to the extent practicable.

Changes to vendor or employee banking information shall be independently verified using a reliable method separate from the original change request before an EFT is released.

EFT transactions shall be supported by appropriate documentation, appropriately authorized, and recorded in the Coalition's accounting records.

EFT activity shall be included in the applicable bank reconciliation and reviewed for unusual, unauthorized, or unsupported transactions.

FA130.08 Stale Checks / Unclaimed Property

Reference Procedure: FA26.130.08 V1.0

The Coalition shall maintain procedures to identify, research, resolve, and appropriately account for stale, outstanding, or otherwise unclaimed checks and payments.

Stale or outdated checks shall not be automatically written off solely because they have remained outstanding for an extended period.

Outstanding obligations shall be evaluated to determine whether the payment remains valid, should be stopped and reissued, should remain outstanding, or is subject to applicable unclaimed-property reporting or remittance requirements.

The Coalition shall exercise due diligence to locate intended payees and resolve outstanding obligations in accordance with applicable accounting principles, funding source requirements, DEL requirements, and applicable Florida law.

The Coalition shall maintain adequate documentation of efforts to contact payees, stop payments, void and reissue checks, resolve outstanding obligations, and report or remit unclaimed property when required.

FA140 – Revenue and Grant Management

FA140.01 Revenue Recognition

FA140.02 Grant Management

FA140.03 Restricted Funds

FA140.04 Allowable Costs

FA145 – Parent Fees and Copayments

FA145.01 Sliding Fee Scale

FA145.02 Copayment Collection

FA145.03 Copayment Adjustments

FA150 – Purchasing and Procurement

FA150.01 Procurement Principles

FA150.02 Purchasing Authority

FA150.03 Competitive Procurement

FA150.04 Vendor Management

FA150.05 Contract Administration

FA160 – Accounts Payable and Disbursements

FA160.01 Accounts Payable Procedures

FA160.02 Invoice Processing
FA160.03 Payment Authorization
FA160.04 Electronic Payments
FA160.05 Prepaid Costs

FA165 – Provider Payments
FA165.01 Provider Payment Schedule
FA165.02 Attendance Verification
FA165.03 Payment Adjustments
FA165.04 Overpayment Recovery

FA170 – Payroll Processing
(Compensation rules are governed by HR Policy)
FA170.01 Payroll Processing
FA170.02 Payroll Controls
FA170.03 Payroll Tax Compliance

FA180 – Travel and Expense Reimbursements
FA180.01 Travel Authorization
FA180.02 Allowable Expenses
FA180.03 Mileage Reimbursement
FA180.04 Expense Documentation

FA190 – Asset and Property Management
FA190.01 Capital Assets
FA190.02 Asset Inventory
FA190.03 Depreciation
FA190.04 Asset Disposal

FA210 – Audits and Financial Compliance
FA210.01 External Audits
FA210.02 Internal Audits
FA210.03 Audit Findings and Corrective Action

FA220 – Records Retention
FA220.01 Financial Records Retention
FA220.02 Secure Storage
FA220.03 Records Destruction

FA230 – Subrecipient and Contract Monitoring
FA230.01 Risk Assessment
FA230.02 Monitoring Procedures
FA230.03 Corrective Actions

FA250 – Policy Compliance
FA250.01 Compliance Monitoring
FA250.02 Policy Violations

Add Risk Management Policy
FA260 – Risk Management

Appendices

Appendix A Financial Definitions

Appendix B Approval Authority Matrix

Appendix C Related Forms

Appendix D Revision History

DRAFT



Action Sheet

FULL COALITION BOARD

October 22, 2026

SUBJECT: ELCMC Organizational Chart for FY 2026 – 2027, Revision 1

FISCAL IMPACT: \$20,542 – \$29,902

PROPOSED ACTION

Approve the revised ELCMC Organizational Chart and associated position changes, effective October 22, 2026.

BACKGROUND INFORMATION

Organizational Structure and Position Changes:

The proposed organizational changes include the following:

- EC Program Director → EC Program Manager: Adjust the position to manager level to reduce personnel costs and provide support for inclusion services.
- Add CSC: Inclusion (Full-Time): Establish a new full-time position to assist the current Inclusion Coordinator with inclusion-related services and EC Program support.
- Remove CSC: Instructional Support Coach: This position is not included in the current budget.
- Remove Professional Development Assistant: This position is not included in the current budget.
- Remove CSC: Reimbursement: This position is not included in the current budget.

Programmatic Impact:

Reclassifying the EC Program Director position to EC Program Manager creates an opportunity to establish a full-time CSC: Inclusion position within the available staffing budget. This additional support will allow the Inclusion Coordinator to dedicate more time to providing inclusion training and technical assistance to providers. Strengthening this capacity will help ELCMC better support providers in meeting the needs of children requiring inclusion services and promote inclusive practices in early learning environments.

Approval of this organizational chart is required to comply with the SR Coalition Plan as outlined by the Division of Early Learning.

Supporting Documentation Included:

- 2026 – 2027 Organizational Chart R-1



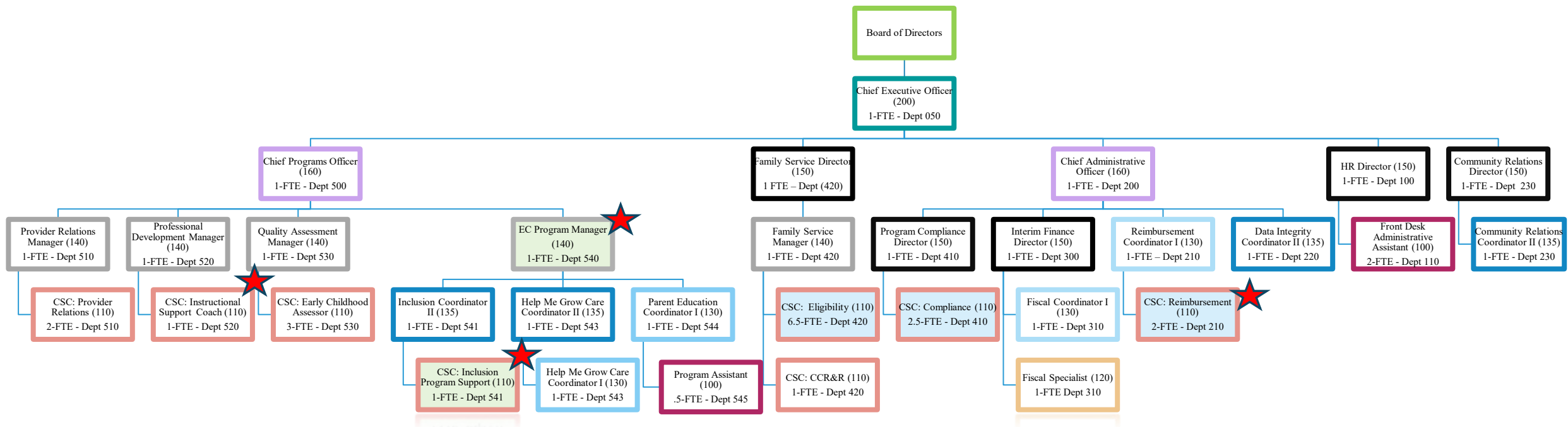
Early Learning Coalition

OF Marion County

Organization Chart

FY2026-2027 R1

-  - Open Position
-  - Proposed Position
-  - Frozen Position



- | | | |
|---|--|--|
|  - Executive Director (200-E) |  Manager (140-E) |  Specialist (120-NE) |
|  - Officer (160-E) |  Coordinator I (130-E) |  CSC: hourly staff (110-NE) |
|  - Director (150-E) |  Coordinator II (135-E) |  Hourly staff (100-NE) |

45 Staff
43.5 FTE

As of 10/22/26- By Position
Updated 10/9/2026 M Easter
Approved by Exec: TBD 1
Approved by Board:TBD

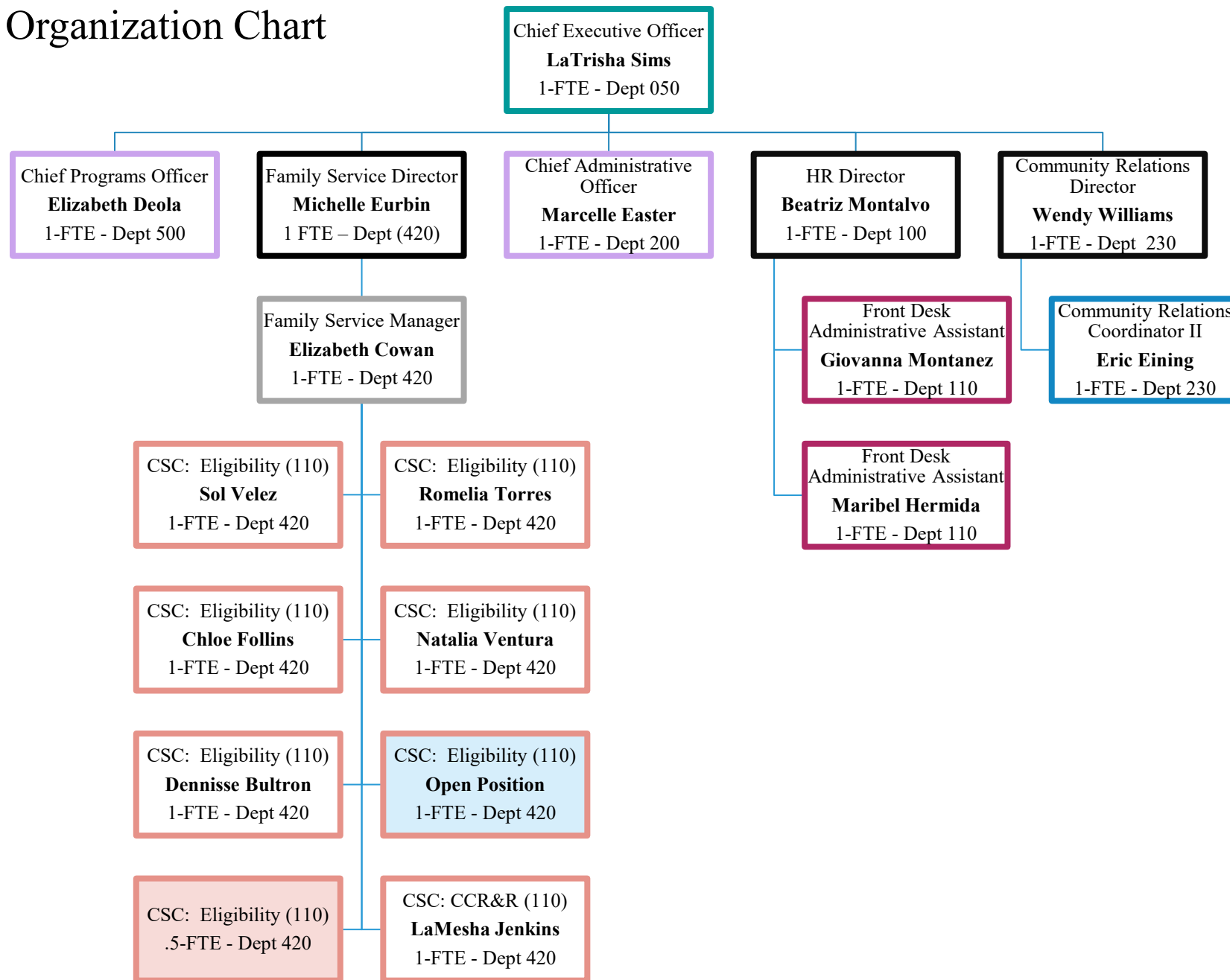


Early Learning Coalition

OF Marion County

Organization Chart

- Open Position
- Proposed Position
- Frozen Position



- Executive Director (200-E)
- Manager (140-E)
- Specialist (120-NE)
- Officer (160-E)
- Coordinator I (130-E)
- CSC: hourly staff (110-NE)
- Director (150-E)
- Coordinator II (135-E)
- Hourly staff (100-NE)

As of 10/22/26- CEO – by Name
Updated 10/9/2026 M Easter
Approved: TBD



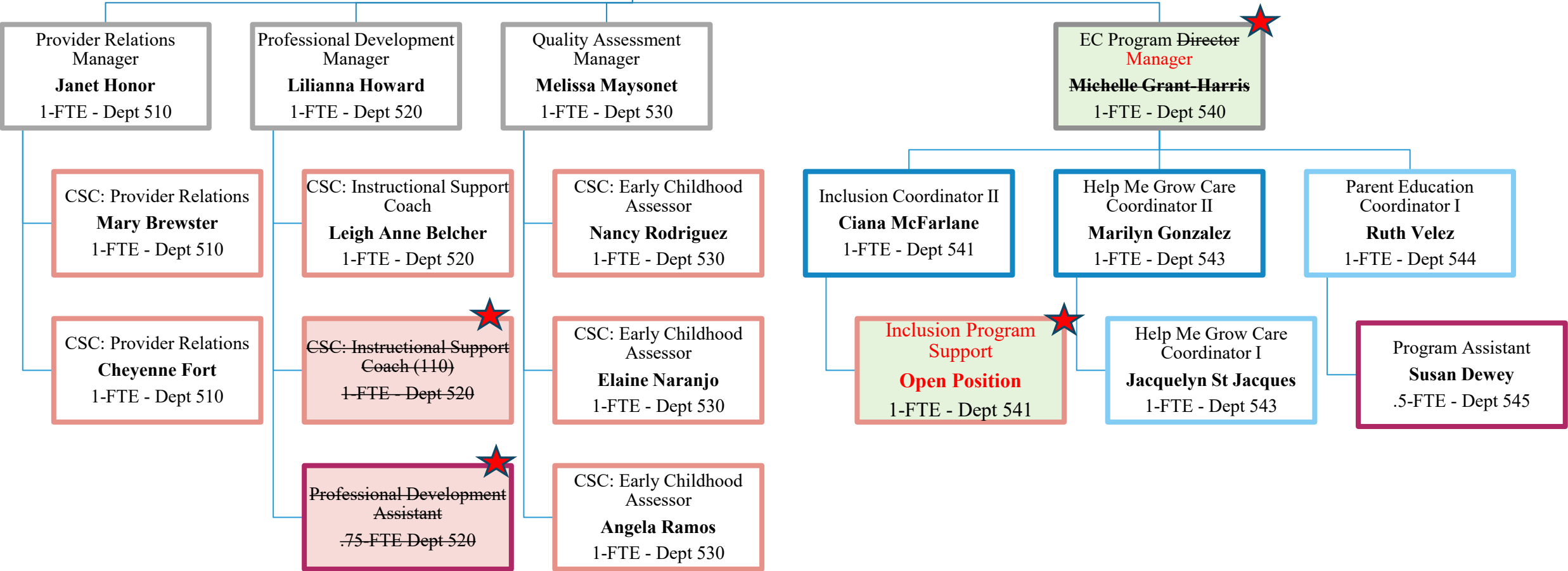
Early Learning Coalition

OF Marion County

Organization Chart

- Open Position
- Proposed Position
- Frozen Position

Chief Programs Officer
Elizabeth Deola
1-FTE - Dept 500



- | | | |
|--|--|--|
| - Executive Director (200-E) | Manager (140-E) | Specialist (120-NE) |
| - Officer (160-E) | Coordinator I (130-E) | CSC: hourly staff (110-NE) |
| - Director (150-E) | Coordinator II (135-E) | Hourly staff (100-NE) |

As of 10/22/26- Programs by Name
Updated 10/9/2026 M Easter
Approved: TBD

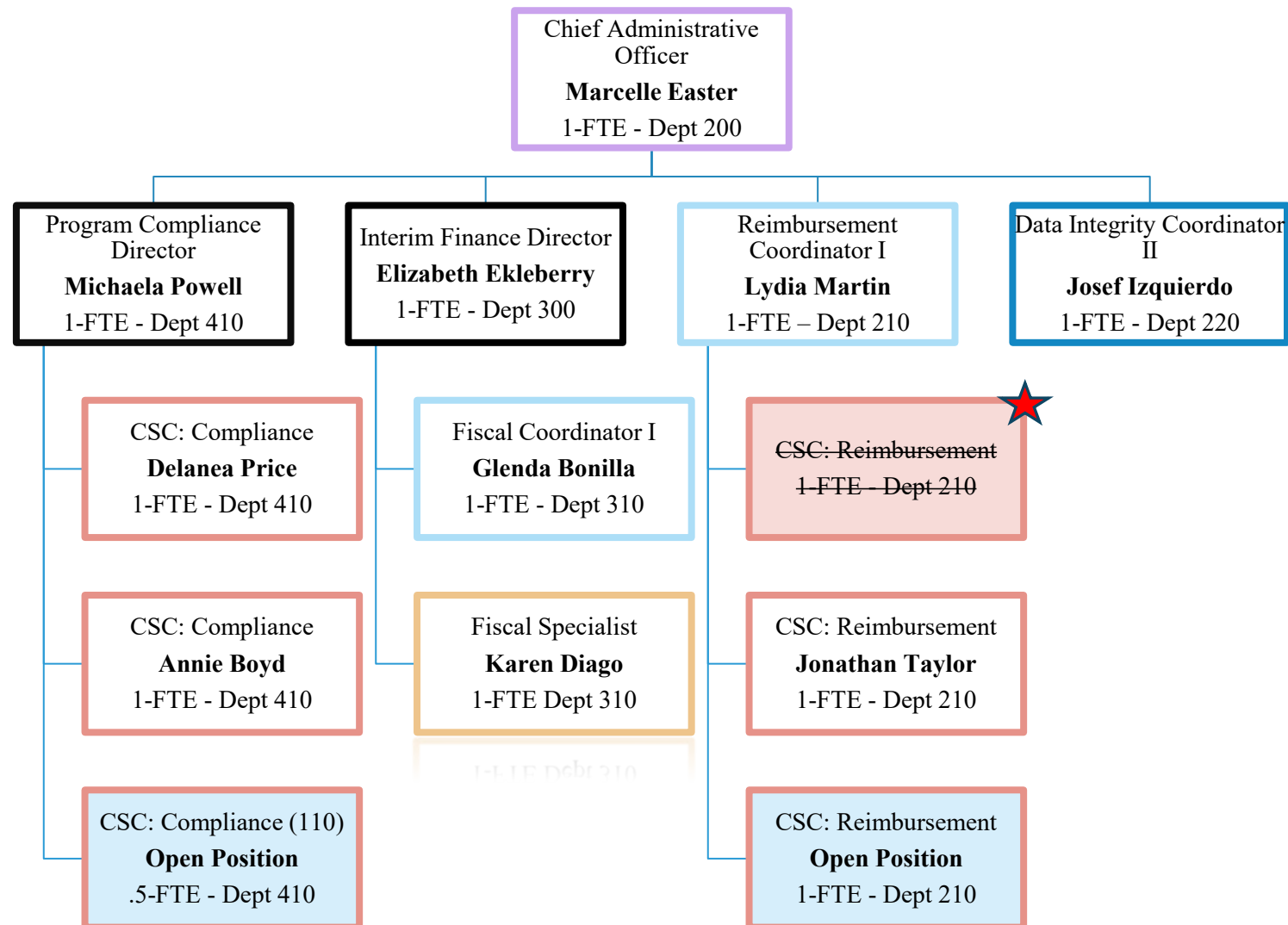


Early Learning Coalition

OF Marion County

Organization Chart

- Open Position
- Proposed Position
- Frozen Position



- Executive Director (200-E)
- Officer (160-E)
- Director (150-E)
- Manager (140-E)
- Coordinator I (130-E)
- Coordinator II (135-E)
- Specialist (120-NE)
- CSC: hourly staff (110-NE)
- Hourly staff (100-NE)

As of 10/22/26- Admin by Name
Updated 10/9/2026 M Easter
Approved: TBD

Information Items



EARLY LEARNING POLICY ROADMAP

Investing Today for Brighter Tomorrows

CHILDREN
FAMILIES
STRONGER COMMUNITIES
A BRIGHTER FLORIDA

2027–2028

2029–2030

2031+

SR Eligibility

- Expand access to School Readiness from 0–85% of State Median Income.
- Create a seamless continuum of care with graduated parent copays.
- Strengthen parent choice and support family economic mobility.

Provider Reimbursement Rates

- Increase provider reimbursement rates to better reflect the cost of care.
- Strengthen the early learning workforce and support competitive teacher pay.
- Improve provider stability and protect families' access to early learning.

Shift Nonrecurring Pots for Quality Performance Incentive and Gold Seal to Recurring Funding

- Move Quality Performance Incentive and Gold Seal funding from nonrecurring to recurring.
- Create stable, predictable funding for quality incentives.
- Strengthen the long-term sustainability of Florida's quality early learning system.

Increased Investment and Access to Early Childhood Education

- Increase state investment in early childhood education.
- Expand access and support the early learning workforce.
- Drive economic mobility and improve kindergarten readiness for all children.

Additional Priorities

- To be determined.

Additional Priorities

- To be determined.



A high-quality, accessible, and sustainable early learning system that prepares every child for success in school and in life.

STRONG
FOUNDATIONS.
BRIGHTER
FUTURES.



À LA CARTE OPPORTUNITIES (ALL YEARS)



Parenting Plan/
Child Support
Enhancements



VPK Quality
Differentials



Increased SR
Quality Differentials



Online Testing for
DCF Intro Courses



DCF Licensing
Ratios for 2-Year-Olds



2 Year
Grant Cycle



Revert &
Reappropriate



Fund
Balance



Reop/Deob
Flexibility

CHILDREN THRIVE

FAMILIES SUCCEED

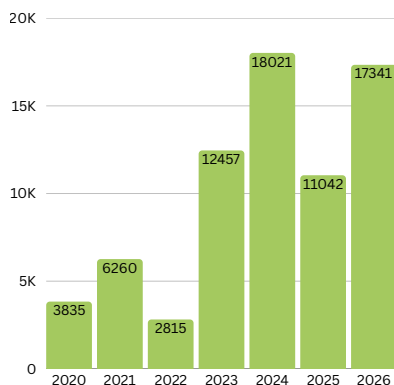
COMMUNITIES GROW

FLORIDA PROSPERS



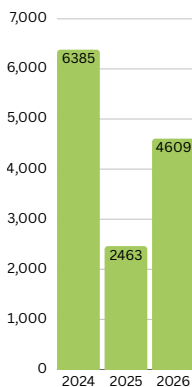
2026 Results

Donations



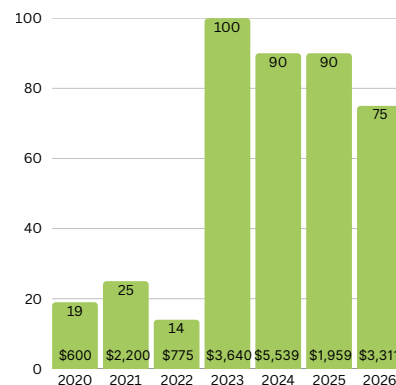
2026 Goal: Raise \$15,000
2026 Actual: \$17,341

Advance Funds



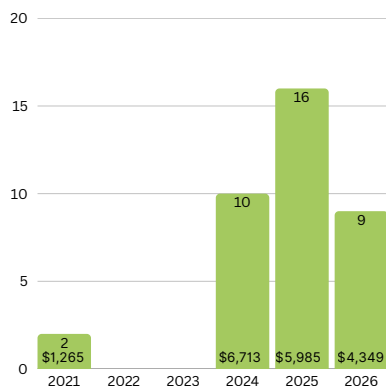
2026 Goal: \$5,000 in Advance
2026 Actual: \$4,609

Percent Board Giving



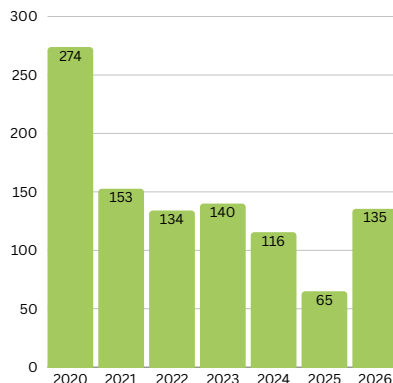
2026 Goal: 100% Board Giving
2026 Actual: 75%

Peer-to-Peer Friendraisers



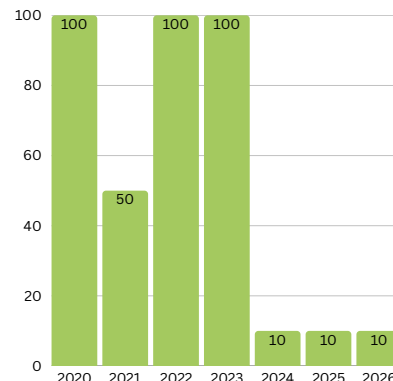
2026 Goal: 20 Friendraisers, at least 1 Board Member
2026 Actual: 9 Friendraisers, 0 Board Members (brought in 36 new donors)

Average Donation Per Donor

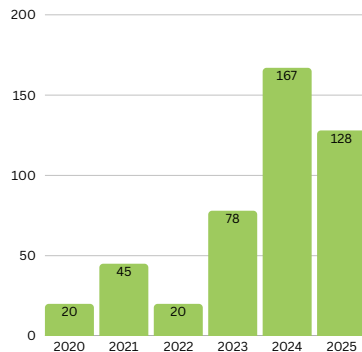


2026 Goal: \$100 Avg. Donation per Donor
2026 Actual: \$135.48

Most Frequent Donation Amount

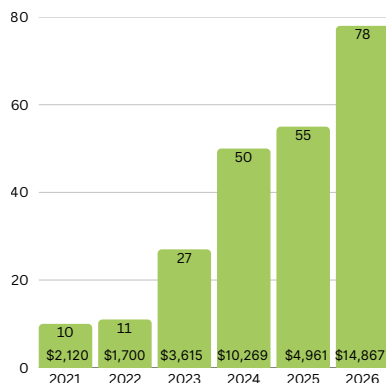


Individual Donors



2026 Goal: 175 Individual Donors
2026 Actual: 128

Repeat Donors



2026 Goal: 60 Repeat Donors
2026 Actual: 78 (30 increased gift, 29 decreased, 19 stayed the same)

New Donors





**Early Learning
Coalition** Marion
County

Early Learning Coalition of Marion County

2025-2026 ANNUAL IMPACT REPORT

Mission: Equip every young child and family for success

ELC-Marion.org • 2300 SW 17th Rd, Ocala, FL 34471 • (352) 369-2315



Letter from the CEO

Reflecting on the 2025–2026 fiscal year, I am grateful for the dedication and partnership of our Board of Directors, staff, early learning providers, community partners, funders and the families we are honored to serve.

Together, we expanded access to high-quality early learning opportunities, strengthened support for families, and continued the work to ensure every child enters school ready to learn and succeed. We helped more than 5,500 children access early learning programs and supported 166 providers in strengthening the quality of care they offer. These achievements reflect our community's shared commitment to our mission to equip every young child and family for success.

We remain committed to stewarding resources responsibly and investing in strategies that strengthen families, support our workforce, and create a thriving community.

Thank you for your partnership and support. Together, we are creating brighter futures for Marion County's children and families.

With sincere appreciation,



LaTrisha Sims
Chief Executive Officer



Support Our Work

Creating brighter futures for children and families takes a community effort. We invite individuals, businesses, and organizations to partner with us by:

- Making a financial contribution
- Sponsoring our early learning initiatives
- Hosting a diaper drive
- Volunteering
- Sharing our mission
- Advocating for young children

**SCAN
TO
LEARN
MORE**

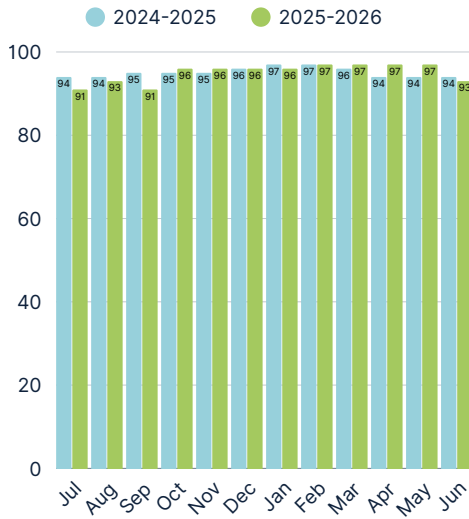


Your support helps expand opportunities for children, strengthen families, and build a stronger Marion County.

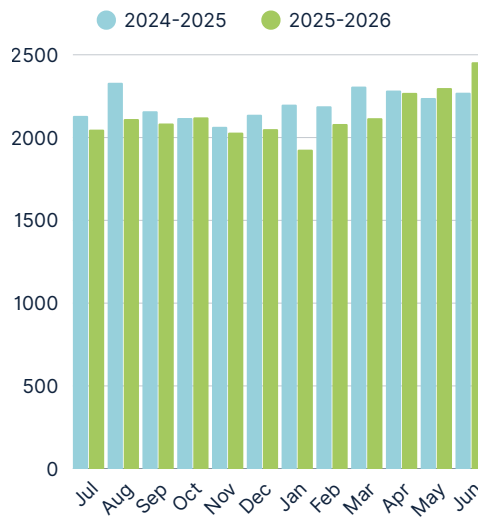


SCHOOL READINESS (SR)

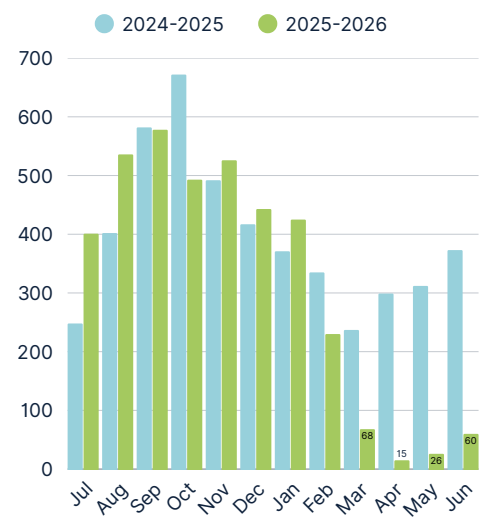
Child Care Providers



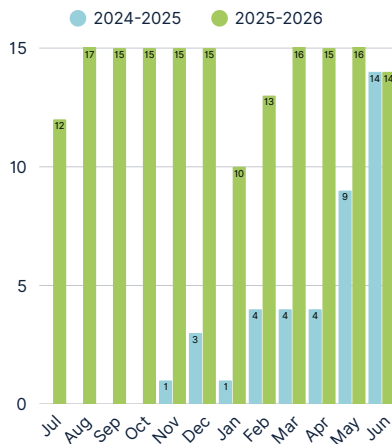
Children Served



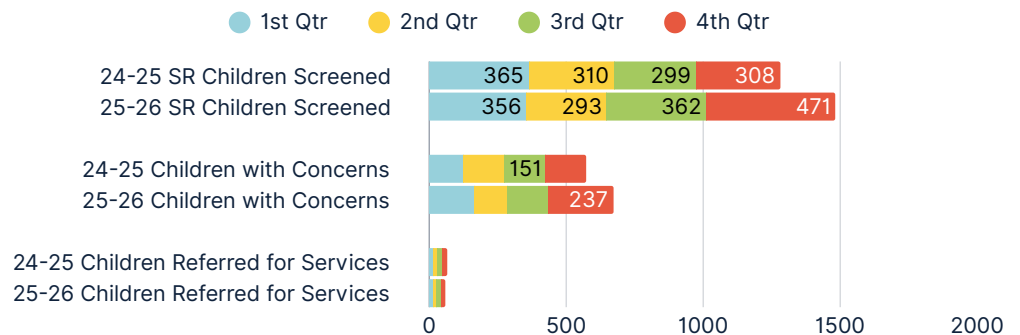
Waitlist



SR Plus Children Served



Inclusion



The Florida School Readiness (SR) program provides child care financial assistance to eligible families with children birth to 13. Child care providers meeting specific quality, health, and safety standards contract with the Coalition to provide SR services.

The SR waitlist is based on funding and provider availability.

The SR Plus program went into effect on September 24, 2024, and provides financial assistance to low-income SR families who are no longer eligible for the full SR subsidy.

Participating children are screened for developmental delays. The Coalition's Inclusion Coordinator reviews any concerns with parents or guardians and encourages their consent for referral to supportive services.

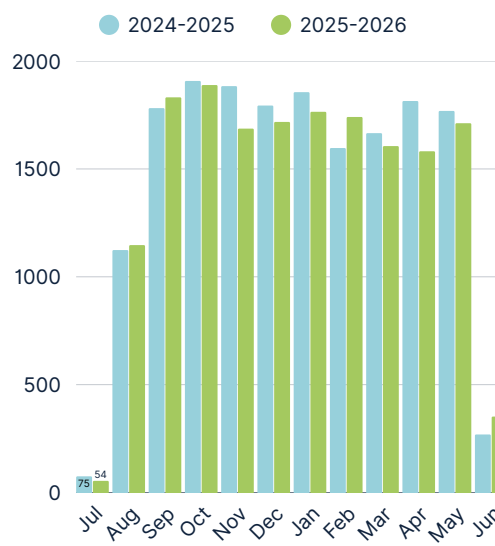
2025-26 COMMUNITY IMPACT REPORT CONTINUED

VOLUNTARY PREKINDERGARTEN

Child Care Providers

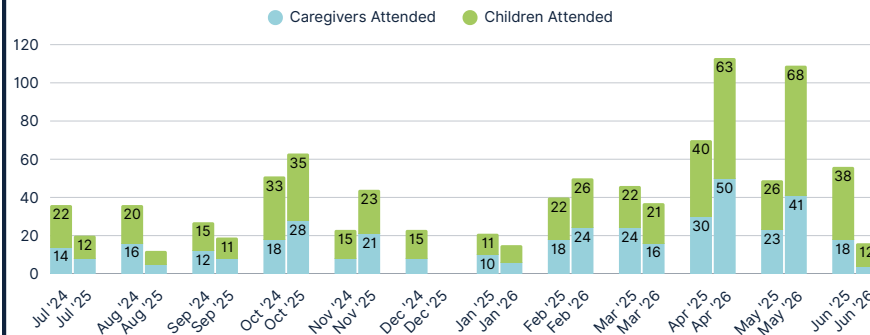


Children Served



Florida's Voluntary Prekindergarten (VPK) program is a free, high-quality education program for all four- or five-year-old children who have not entered kindergarten. Contracted VPK providers meet quality standards and performance metrics.

KALEIDOSCOPE PLAY & LEARN



Kaleidoscope Play & Learn is a free weekly play group for children birth to five and their parent or caregiver. Children learn socialization skills while caregivers learn ways to support children's learning and healthy development at home.

82% of KPL survey respondents reported increasing their knowledge about:

- Their role in helping children prepare for school
- What to expect of children of different ages
- How children learn through play

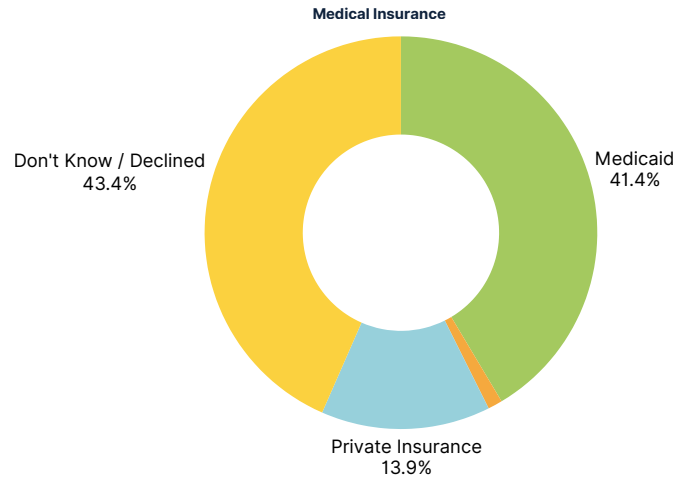
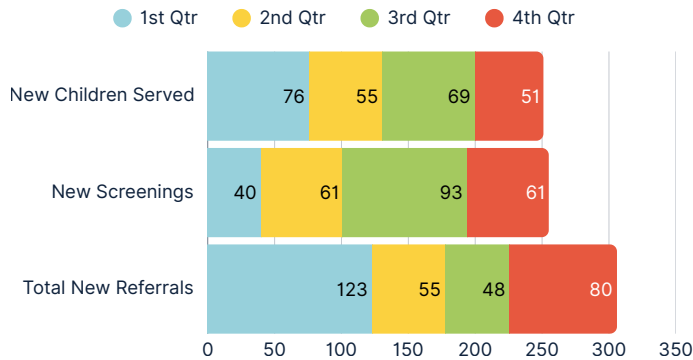
THE INCREDIBLE YEARS®

Fall	Spring	
16	18	Parents / Guardians Enrolled
10	9	Parents / Guardians Graduated
90%	89%	of program graduates reported a decrease in the frequency of their child's problematic behaviors
100%	88%	of program graduates reported improved or greatly improved confidence in their ability to manage future behavior problems

The Incredible Years® Preschool Parenting Program assists families with children three to five years old. In 14-week sessions, parents learn to minimize challenging behaviors and help their preschoolers improve their social skills and communication.

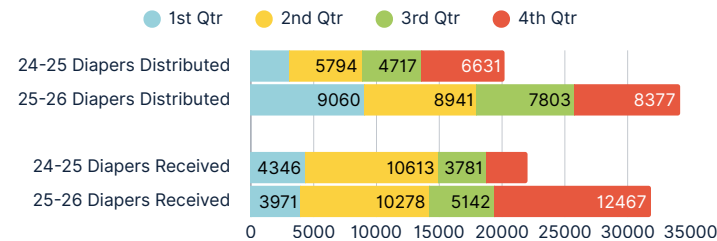
2025-26 COMMUNITY IMPACT REPORT CONTINUED

HELP ME GROW



Help Me Grow supports healthy development for children birth to eight. Free screenings help identify developmental and behavioral concerns. Care coordinators provide families with customized support and connections to community services for early intervention. Coordinators also help families navigate any barriers to accessing care and support.

DIAPER ASSISTANCE



279

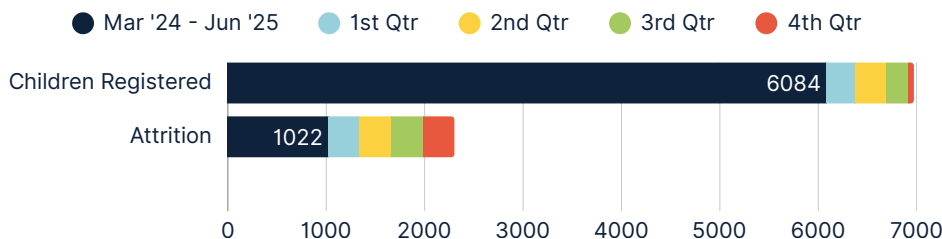
Families (compared to 196 in 2024-2025)

11

Organizations

Emergency diaper assistance is provided to eligible families, helping to meet a basic health need while reducing barriers to child care and employment. This program is 100% supported by community donations.

DOLLY PARTON'S IMAGINATION LIBRARY



4,670 Active Registrations

109,852 Books Mailed since Program Launch

Launched County wide in March 2024, Dolly Parton's Imagination Library mails a free, high-quality, age-appropriate book each month to registered children ages birth to five.

Survey results show participating families read more frequently with their children - a key to improving kindergarten readiness and reading scores.

2025-26 COMMUNITY IMPACT REPORT CONTINUED

CHILD CARE QUALITY INITIATIVES

780 Teachers Attended Coalition Trainings (includes duplicates)

The Coalition provides high-quality training opportunities to early childhood educators contracted to provide School Readiness or VPK programs.

VPK Performance Metric and Designation

Designations	School Year		Summer	
	Percent of Providers	Provider Count	Percent of Providers	Provider Count
Excellent	43%	40	33%	1
Above Expectation	28%	26		
Meets Expectation	25%	23	33%	1
Below Expectation	1%	1	33%	1
Unsatisfactory	0%	0		
Incomplete	3%	3		

The Florida Department of Education VPK performance metrics and designations measure quality, achievement, and learning gains based on classroom observations and student progress monitoring assessments.

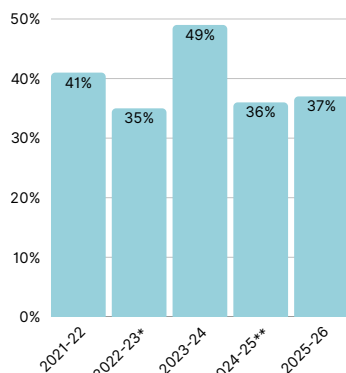
The Classroom Assessment Scoring System® Score (CLASS®) Matrix

July 1, 2025 - June 30, 2026

Overall Score	SR Providers	VPK Providers	Total Providers
6.5 and above	0	2	2
6 to 6.49	1	14	15
5.5 to 5.99	15	33	41
5 to 5.49	36	38	64
4.5 to 4.99	19	7	22
4 to 4.49	1	0	1
3.5 to 3.99	0	0	0
Total	72	94	145

Coalition certified observers measure high-quality interactions between teachers and children in School Readiness and VPK classrooms, using the CLASS® tool. Higher scores reflect more effective interactions. Technical assistance is provided to sites needing improvement. Sites must score at least a 4 to remain contracted with the Coalition.

KINDERGARTEN READINESS



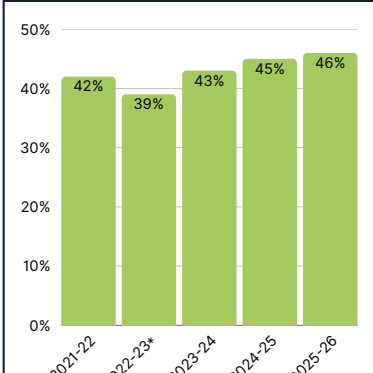
*2022-23 was first year of new FL Assessment of Student Thinking (FAST) Star Early Literacy screening and progress monitoring system
 **Kindergarten Readiness cut score increased in 2024-25

Kindergarten Readiness rates indicate the percent of Marion County children ready for school based on a screening administered to public school students in the first 30 days of kindergarten. Research from the Florida Chamber Foundation indicates that 75% of children who are not school ready when they enter kindergarten never catch up.

Third Grade Reading scores indicate the percent of Marion County students reading at or above a third grade reading level based on a screening administered to public school and some private school students in the last month of third grade.

Kindergarten Readiness and third grade reading scores are community health indicators. When children enter kindergarten ready, they are more likely to read proficiently by third grade, graduate on time, succeed in the workforce, and contribute meaningfully to the economy.

THIRD GRADE READING

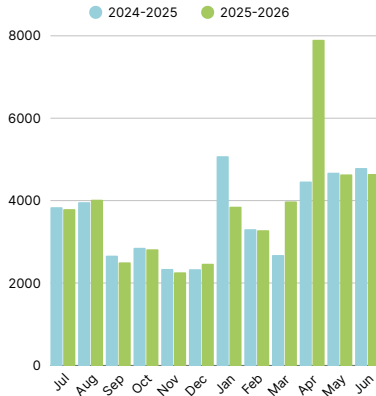


*2022-23 was first year of new FL Assessment of Student Thinking (FAST) Star Early Literacy screening and progress monitoring system

2025-26 COMMUNITY IMPACT REPORT CONTINUED

COMMUNITY OUTREACH

Website Users



The Coalition uses both digital and in-person activities to inform the community about our services and the importance of quality early learning opportunities.

In-Person Outreach

28

Community events attended to promote programs and services to families and partners

6

Presentations to community partners, families, and business leaders

5,121

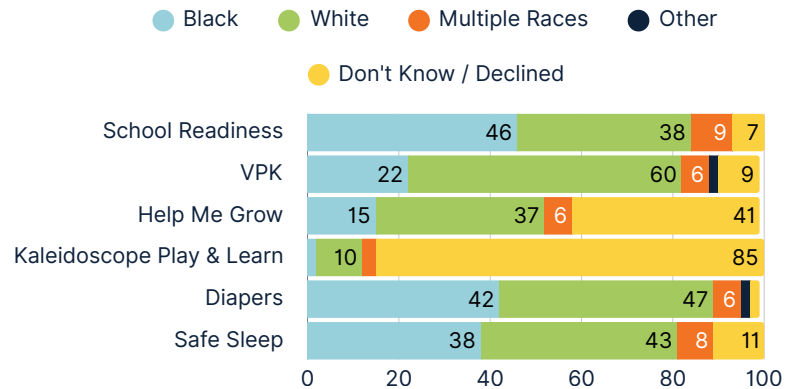
Books Distributed

Social Media

	Social Media Followers	Follower Percent Change	# of Engagements
Facebook	3,801	+9%	7,790
Instagram	595	+8%	398
YouTube	436	-1%	1,123
LinkedIn	206	+13%	50

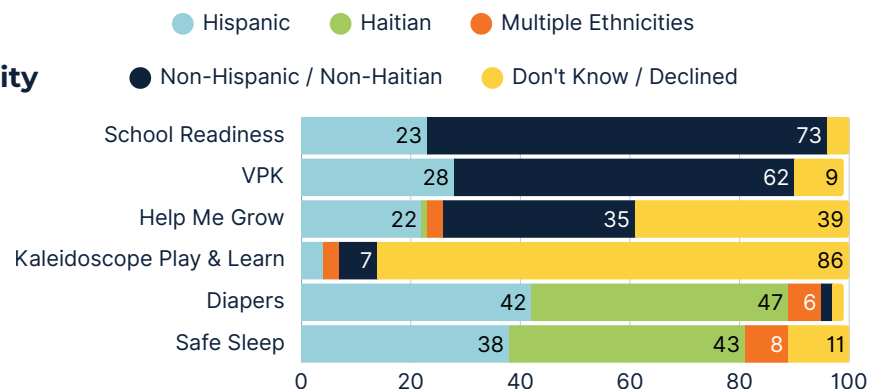
PROGRAM DEMOGRAPHICS

Percent of Program Participants by Race



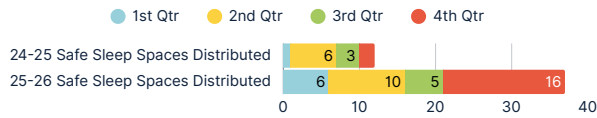
The Coalition analyzes program demographics to ensure equity and identify service gaps.

Percent of Program Participants by Ethnicity



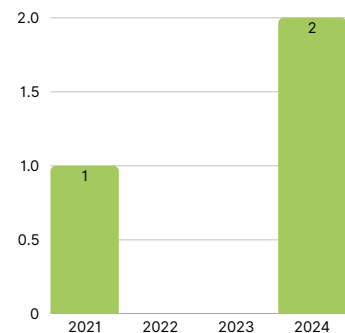
2025-26 COMMUNITY IMPACT REPORT CONTINUED

SAFE SLEEP



To reduce the risk of suffocation and Sudden Infant Death Syndrome (SIDS), portable cribs and safe sleep education are provided to eligible families who lack a safe sleeping space for their infants.

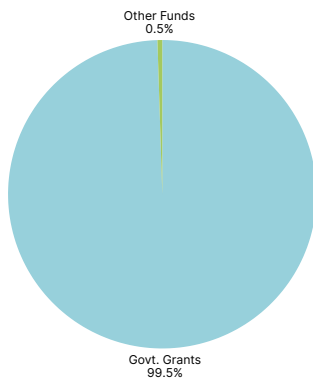
COUNTY SIDS DEATHS



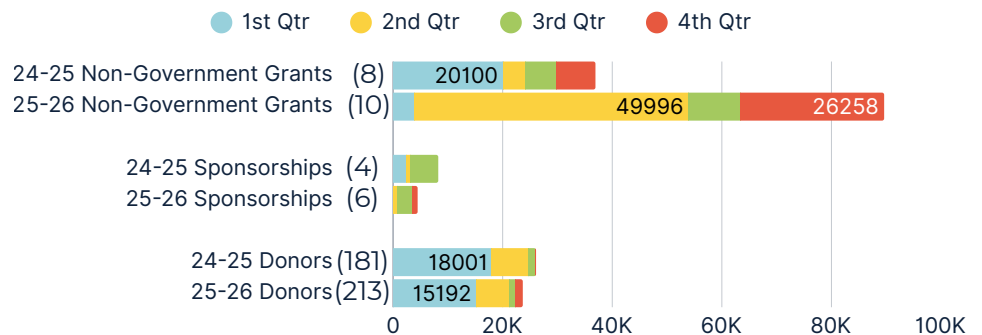
FINANCES

2025-2026 Budget: \$23.4 million

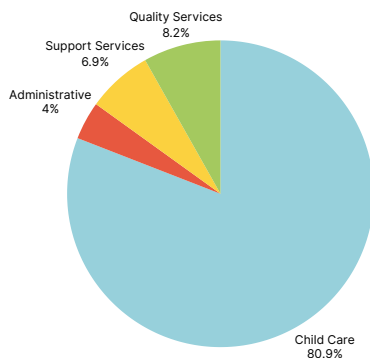
Funding Sources



Other Funds Breakdown



Expenditures



State Expense Mandates

Category	Budget Targets/Restrictions	Actual
School Readiness (SR) Direct Services (Child Care)	Min. 78%	81%
Administrative	Max. 5%	4%
SR Admin., Support, Quality	Max. 22%	18%
SR Quality	Min. 4%	7%